Merchant Card Processing

Authority: G.S. 66-58.12 providing access through Electronic and Digital transactions; fees authorized
G.S. 14-113.24 Credit, charge, or debit card numbers on receipts
G.S. 143B-426.39 Powers and duties of the State Controller
G.S. 147-86.10 Maximization of Receipts, including electronic payments
G.S. 147-86.22 Fees Related to Electronic Payment Processing
G.S. 66-58.12 Electronic and Digital Transactions, fees authorized

History:
First Issued: October 31, 2006
Last Revised: November 1, 2013

Related Documents:
ECU Cash Management Plan
ECU Payment Card Processing Compliance — REG07.60.01

Additional References:
OSC Statewide Electronic Commerce Program

Contact: E-Commerce Manager, 252-737-4729

Note: Some files linked within this document may not be viewable without additional security access.

1. Introduction

The NC Office of the State Controller (OSC) has issued an E-Commerce Policy entitled Maximization of Electronic Payment Methods.” The policy states, in part, “When developing agency cash management plans, each state agency shall consider utilizing electronic payment methods, for both outbound and inbound payments….Each Agency and university shall consider the feasibility of accepting payments via credit/debit card (merchant cards) when appropriate, considering the volume and frequency of payments received.”

East Carolina University (hereinafter referred to as ECU) has determined that it is appropriate to accept merchant cards as an acceptable form of payment for certain types of receipts as described herein. Desirous of developing policies and procedures to ensure compliance with all applicable rules, regulations, and policies associated with merchant cards, the policies and procedures described herein have been adopted. Authorization for Merchant Card Transactions

2. Types of Receipts and Types of Cards Accepted

Receipts:
In its normal course of business ECU accepts merchant cards for the following types of receipts:
Orientation fees, admission fees, parking and transportation fees (citations, permits, and parking), tuition and related fees, housing charges, dining charges, student health fees, donations, event/program registrations, textbooks and other items sold at the University’s bookstore, patient medical and dental charges and ticket sales for both performing arts and athletic events.

In the case of multiple divisions within ECU, approval for the acceptance of merchant cards must be obtained from the Vice Chancellor for Administration and Finance. This responsibility
is delegated to Financial Services and specifically to the Director of Compliance Management. This position supervises the E-Commerce Manager.

Cards Accepted:

In its normal course of business ECU accepts the following merchant cards: VISA®, MasterCard®, Diners Club® and American Express®. When an application for a merchant id is submitted to Office of State Controller, the type of cards that will be accepted by that particular merchant id is specified on the application.

Effective July 2010, ECU outsourced credit card payment processing for the University Cashier's Office to TouchNet for the payment of tuition, fees, and other student related charges consolidated on student accounts. TouchNet's PayPath payment card processing service accepts the following merchant cards: MasterCard®, Diners Club®, American Express®, Discover® and Discover affiliated cards. Recently, VISA® decided to allow percentage convenience fee charges (as opposed to a flat amount) on VISA transactions. Effective with the contract addendum dated July 31, 2013 ECU now accepts VISA payments... The University Cashier’s office continues to accept PIN based debit cards only in the office. Types of Merchant Cards Accepted

3. Transaction Fees

ECU does not levy a transaction fee (surcharge) for any face-to-face (card-present) transactions. Charging Transaction Fees

ECU received approval from the Office of State Budget and Management (OSBM) to utilize TouchNet’s payment card processing service on May 18, 2010 - which includes charging a 2.75% transaction fee – for online payments for student fees including tuition, fees, housing, and dining and other charges consolidated to student accounts. The May 18, 2010 memo also served as ECU’s specific approval to charge a transaction fee for cashier online payment card processing. This approval is in accordance with OSC’s guidance on “Charging Transaction Fees” as referenced in the preceding paragraph and in accordance with G. S. 66-58.12.

ECU does not retain any portion of the transaction fee levied by TouchNet.

ECU requires TouchNet to ensure its practices related to charging the transaction fee do not violate any merchant card associations’ rules.

The ECU Registrar’s Office utilizes the AVOW transcript system. Current students and alumni access the AVOW system on line, request a transcript and pay for the transcript online. A convenience fee is charged. The Registrar’s office plans to end this contractual relationship effective December 31, 2013 and is currently in contract negotiations with another vendor to provide this same service. The proposed contract is currently being reviewed for both PCI and Cash Management compliance.

The ECU Athletics Ticket Office, Theatre & Dance and Central Ticket Office utilize Paciolan Ticketing Software to issue tickets to events. Paciolan Ticketing software can be accessed for both seating/admission selection and payment on line. Paciolan assesses ticket fees related to
ticket production, printing and delivery. The order fee covers costs such as postage, printing, and other ticket production costs. The Paciolan system assesses the ticket fees based on the nature of the event and ticket production methodology (print at home, in person or mailed); the fees are not charged based on the payment type.

ECU does not charge a transaction fee for accepting payment cards on line for any other payment card activity for any other merchant id other than the University Cashier’s On-line payment system – which is outsourced to TouchNet.

4. Funding to Pay Costs

ECU adheres to all requirements pertaining to the securing of funding to pay for costs associated with processing merchant cards, including internal costs and cost paid to third party processors.

Merchant fees for credit card processing are treated as an expense to the department where the revenues were generated. State appropriations are used to pay merchant fees attributed to state receipts as referenced in G.S. 147-86.22. Institutional funds are used to pay merchant fees attributed to institutional receipts.

Any expenses associated with programming and maintaining ECU’s OneStop are funded from ECU’s Information, Technology and Computing Services’ department operating budget.

The East Carolina University Foundation and the ECU Medical and Health Sciences Foundation are charged merchant fees based on their respective merchant id activity. The East Carolina University Foundation allocates fees internally as donations are received to appropriately charge the expense of collecting the donation to the fund(s) where the revenue is recorded. The ECU Medical and Health Sciences Foundation is in the process of instituting a similar cost allocation process.

Funding for Electronic Payment Services

5. Methods of Capture

POS Terminals (stand-alone card readers): used primarily for card-present transactions (card swiped.) POS Terminals are also used for card-not-present transactions such as mail orders and telephone orders and the required information to process the charge is manually keyed. All POS Terminals use dedicated analog telephone lines except for those newer machines that would not process properly on the analog lines. POS terminals for Parking and Transportation and for the One Card Office are on the PCI VLAN behind the firewall. All POS terminals and applications have been self-assessed and found to be PCI compliant.

Local Application - connecting to Third Party Gateway: used for card present and card-not-present transactions. Paciolan® is utilized for Athletics, Central Ticket Office, Theatre and Dance, and Educational Foundation (Pirate Club.) Paciolan utilizes Protobase 6.01 as its payment gateway. VeriFone-PAY ware is utilized for Campus Recreational & Wellness Services
and VeriFone is also utilized by Dowdy Student Stores. Authorize.net is also utilized for Athletics on-line ticket sales and Educational Foundation (Pirate Club). CFNC utilizes VeriSign.

Internet Application – hosted by third party: TouchNet is used as the ECU’s primary third party gateway for all applications unless referenced in the preceding paragraph.

Common Payment Service (CPS) gateway: used on campus for those locations not set up to process transactions via TouchNet or other approved third party gateways. Currently, CPS is not utilized by any campus activities.

6. Third Party Service Providers

Merchant Card Processing Services:
The State of North Carolina has a Master Services Agreement (MSA) with SunTrust Merchant Services (STMS), which is affiliated with First Data Merchant Services (FDMS). STMS provides merchant card payment processing services to state and local government entities on a statewide enterprise basis.

On November 1, 2006 ECU obtained approval to participate in the OSC Master Services Agreement (MSA) with STMS, as required by OSC’s E-Commerce policy entitled “Master Services Agreements for Electronic Payments.” Accordingly, the Vice Chancellor for Administration and Finance executed an Agency Participation Agreement (APA) allowing ECU to subscribe to the MSA as a “participant.” The APA was reviewed before execution by ECU’s management, and management is aware of the responsibilities and obligations required by the terms of the APA, and by reference, the terms of the APA, and by reference, the terms of the MSA. ECU’s copy of the executed APA is filed in the office of the E-Commerce Manager.  

Master Services Agreement

Payment Gateway Services:
The Common Payment Service (CPS) is the State’s payment gateway used for Internet merchant card transactions. OSC has mandated that all State entities subject to the State Cash Management Law use CPS unless an exemption has been approved.

On November 1, 2006, ECU obtained approval to participate in the CPS, as required by OSC’s E-Commerce policy entitled, “Master Services Agreements for Electronic Payments.”

A third-party gateway service provider may also be utilized, provided it is one pre-approved by OSC. Some gateway providers offer a capture solution that also has a “presentment engine” (in addition to the “payment gateway”), which provides hosting of the university’s website. Some gateway providers cannot use SunTrust Merchant Services as the processor / acquirer, but use their own processor / acquirer. ECU has requested and been approved to use TouchNet® as its primary payment gateway. ECU has also requested and been approved to use other third party gateways that are application specific: Paciolan® Protobase Elavon 6.01, Digital ® Pay Technologies, and VeriPhone® Pay Technologies.

Payment Applications:
Capture solutions utilizing POS Software applications are obtained from vendors that have had the application (version utilized) validated as being compliant with the PCI Payment Application Data Security Standard (PCI PA-DSS), formerly known as Visa’s “Payment Application Best Practice” (PABP). The payment application must be listed either on Visa’s “List of Validated Payment Applications,” or on the PCI Council’s website.

[PCI SSC Date Security Standards Overview]
[VISA List of PABP Validated Payment Applications]

**ECU as a Service Provider:**
Due to ECU’s relationship with Aramark which includes ITCS maintaining Aramark’s firewall, ECU functions as a Service Provider to Aramark.

Due to ECU’s Central Ticket Office offering on-line and credit card sales for non ECU ticketed events on ECU’s campus, ECU functions as a Service Provider to those various entities.

**Other Service Provider:**
ECU’s Alumni Association contracts with DirectLine Technologies, INC to solicit memberships for the Alumni Association during its annual membership campaign drive. In the course of soliciting the memberships, DirectLine collects credit card information on behalf of ECU’s Alumni Association. ECU is in the process of terminating this contractual relationship.

ECU is currently negotiating a contract with Credentials INC to provide electronic transcripts to students, alumni and others where authorized. In the course of completing a transcript request, Credentials will collect credit card information on behalf of ECU’s Registrar’s Office. Contract details are being finalized with a target implementation date of January, 2014.

7. **Proprietary Card Companies**

ECU elected to accept American Express® for certain merchant activity and entered into a master agreement maintained by the OSC.  **Types of Merchant Cards Accepted**

On April 1, 2008, the Vice Chancellor for Administration and Finance executed an Agency Participation Agreement (APA) allowing ECU to subscribe to the Master Agreement with American Express as a “participant.” The APA was reviewed before execution by ECU’s management, and management is aware of the responsibilities and obligations required by the terms of the APA, and by reference, the terms of the Master Agreement. ECU’s copy of the executed APA is filed in the office of the E-Commerce Manager.

8. **Data and System Security:**

**PCI DSS Compliance:**
Each of the merchant card associations has established security standards that all merchants and processors must follow to ensure that cardholder data, as well as the payment network, is protected and kept secure. The standards are referred to collectively as the "Payment Card Industry Data Security Standard (PCI DSS)," which has been issued by the [PCI Security Council]. The primary focus of the PCI DSS is to help merchants (agencies) improve the security of cardholder information by improving overall security standards which reduces the chances of security breaches. The policies and resulting procedures are intended to help ensure that
cardholder data and the electronic commerce network are protected and kept secure, thereby avoiding potential fines. Reference OSC’s Programs section – Payment Card Industry (PCI) Security Compliance Program for more information. 

**Payment Card Industry (PCI) Security Compliance Program**

The most useful document to view is: “PCI Applicability to Capture Methods.”

**PCI Applicability to Capture Methods**

ECU will take all necessary steps to ensure that all merchant card applications (merchant numbers) used by the university are kept compliant with the PCI DSS. ECU will advise OSC, and keep OSC updated with, the name of the agency’s PCI contact. This individual is usually the E-Commerce Manager.

To assist in validating ECU’s compliance with the PCI DSS, ECU has enrolled with Trustwave, OSC’s selected vendor for providing PCI Security Validation Services. Enrollment is at the “chain level” and provides for: 1) an annual Self-Assessment Questionnaire (SAQ) to be completed online; and 2) vulnerability scans required for all capture solutions having external-facing IP addresses (URLs and PC capture software). Scans do apply to ECU’s applications, and all applicable IP addresses have been enrolled with Trustwave to be scanned monthly. The completion of the annual Self-Assessment Questionnaire (SAQ) will be performed each November via Trustwave’s TrustKeeper, and will be the responsibility of the E-Commerce Manager.

Sun Trust Merchant Services (STMS) has assigned ECU unique “chain” merchant numbers for MasterCard® (including Diner’s Club)/VISA® and for American Express®. For security purposes, the chain number and merchant numbers are not listed here.

The university’s chain number is enrolled in TrustKeeper under the following option: SAQ and Vulnerability Scanning. 

**PCI Security Standards Council**

**Compliance with PCI Data Security Standards**

There are five versions of the SAQ that is to be completed, depending upon the capture method and upon whether or not a third-party service provider is utilized.

**PCI DSS Self-Assessment Questionnaire (SAQ)** If multiple outlet numbers are utilized by a university (e.g., multiple divisions) a separate SAQ is to be completed by each division (paper form, not online). Each division may qualify for a different version of the SAQ. Through TrustKeeper, there should only be one SAQ completed online, the version that is the most stringent.

Recently ECU engaged the services of a Quality Security Assessor (QSA) from Trustwave to perform a PCI gap analysis. The QSA was on site in September 2013, and as result of that analysis, ECU was determined to be a service provider. Consequently, ECU plans to submit SAQ-D to Trustwave for ECU’s annual self-assessment starting in November 2014.

ECU has merchant numbers associated with its capture solutions having external facing IP addresses (URLs or POS Capture software) that require monthly vulnerability scans, and are enrolled with Trustwave for the purpose of receiving scheduled monthly scanning. The merchant numbers are not listed here for security purposes.
Cardholder data is not stored in the application. The third-party capture application, Sequoia/Verifone and Paciolan/Protobase 6.01 must be and remain compliant with the PCI PA-DSS. They must be listed on Visa’s CISP website or on the PCI Security Council’s website as a “Validated Payment Application.” Default passwords are not used. The software is updated within 30 days of the release of any security patches.

ECU has merchant numbers that do not require vulnerability scanning, as they do not involve external-facing IP addresses. The merchant numbers are not listed here for security purposes.

In accordance with Requirement 12.8 of the PCI DSS, the third-party gateway vendors, functioning as “service providers,” such as TouchNet, must be and remain PCI DSS compliant. A “written agreement” must be in place with the vendor that specifies the vendor’s PCI data security responsibilities. The written agreement language is contained in the original contract, and additionally in any amendments to the original contract. ECU monitors the vendor’s compliance on an ongoing basis. Evidence of compliance will be obtained from the gateway service provider annually.

**PCI Data Security Standard Validation for Service Providers**

Issues detected by either the Self-Assessment Questionnaires (SAQ), or by Trustwave’s vulnerability scans, or by failure of the service provider to demonstrate compliance, will be brought to the attention of the Vice Chancellor for Administration and Finance and the CIO for Information Technology & Computing Services. A plan for remediation will immediately be developed for each incident of non-compliance detected, and the Office of the State Controller will be advised.

ECU has policies that address the twelve primary requirements of the PCI DSS, categorized as follows:

a) Build and maintain a secure network (Requirements 1 & 2): ECU has segregated a section of its network behind a dedicated firewall to protect cardholder data. This PCI VLAN configuration isolates PCI network traffic from all other general network traffic. ECU does not use vendor supplied defaults for system passwords and for other security parameters. Users are provided guidance and users are required to review and sign an annual PCI Security Awareness Certification.

b) Protect Cardholder Data (Requirements 3 & 4): ECU does not store third –party PANs electronically. ECU encrypts transmission of cardholder data and sensitive information across public networks to remote PCI compliant destinations.

c) Maintain a vulnerability management program (Requirements 5 & 6): ECU uses and regularly updates anti-malware software. ECU does not develop systems and applications that process credit cards.

d) Implement strong access control measures (Requirements 7, 8 and 9): All user access to payment card systems is restricted by user id and access is granted to users on a need-to-know basis. All system users are assigned unique ID’s which are reviewed and purged regularly. Physical access to cardholder data is restricted: merchant copies of payment slips contain truncated card numbers. All other PAN storage is outsourced to PCI – compliant payment processors such as TouchNet.

e) Regularly monitor and test networks (Requirements 10 & 11): ECU tracks and monitors all access to network resources. A QSA (Qualified Security Assessor) performs monthly vulnerability scans of ECU systems.
System Security Requirements for Merchant Card Services:
ECU incorporates the following requirements into its processing of merchant cards:

a) System Settings: ECU changes vendor default security settings prior to installing the system on the network. ECU disables or changes default accounts and passwords prior to installing the system on the network. ECU hardens production systems by removing all unnecessary services and protocols. ECU requires use of its VPN or remote access for administrative access.

b) Stored Data Protection: ECU disposes of sensitive cardholder data in a secure manner when that data is no longer needed. In general cardholder data is destroyed after 36 months (3 years). ECU does not store the full contents of any payment card from the magnetic stripe in any manner. ECU strictly prohibits storage of the card-validation codes (three digit values printed on the signature panel of a card) in any manner. All POS terminals and related systems print truncated payment card numbers when displaying cardholder data. Since payment card data is not stored electronically, there is no longer a need to sanitize account numbers before logging in the audit trail. Access to payment card numbers is restricted to users by application. No bulk merchant card data is stored electronically.

c) Transmitted Data Protection: ECU encrypts transmission of cardholder data and sensitive information across public networks to PCI compliant destinations. ECU does not transmit payment card numbers via email.

d) Anti-Malware Protection: ECU’s Information, Technology and Computing Services monitors and ensures all desktops, laptops, and server computing systems connected to the ECU PCI VLAN have ITCS-supported anti-malware software (preferably the most current version) correctly installed, configured, activated and updated with the latest version of virus definitions before or immediately upon connecting to the network. Updates are managed by ITCS and pushed to users connecting to the network as needed. ECU Antivirus Policy

e) Applications and Systems Security: ECU’s PCI VLAN will be established in accordance with the firewall configurations as specified by requirement number 1 of the PCI DSS. All systems on ECU’s PCI VLAN must be updated with the latest security patches within 30 days of their release. (ECU does not develop software for payment card processing; therefore, sensitive cardholder data sanitization is not applicable.) Any sensitive cardholder data stored in cookies via capture methods described in section 2.5 of the PCI DSS must be secured or encrypted.

f) Account Security: ECU manages merchant account security by requiring users to authenticate at each sign on with a unique user ID and password. Passphrases must be – at minimum eight characters long, contain characters from 3 of the 4 character sets (numbers, lower case letter, upper case letter and special characters). Passwords on ECU merchant systems will expire on a regular basis, no longer than ninety (90) days. ECU requires use of its VPN for remote administrative access. ECU policy prohibits group, shared or generic passwords and user passwords are encrypted. All user accounts are regularly reviewed to ensure that malicious, out-of-date and unknown accounts do not exist. Vendor accounts on ITCS systems are disabled when not in use. Ten failed password attempts result in domain account lockout. User terminations are reviewed weekly by ECU’s ITCS Security. ITCS Security revokes access for terminated employees for enterprise software systems. The list
of terminations is sent to other security managers on campus such as Student and TouchNet so that access can be revoked as well. Management can request that ITCS terminate access immediately on a case by case basis.  

**g) Physical Access:** ECU does not allow PAN’s to be stored electronically on University systems. ECU maintains a listing of all devices used to process credit card data. Multiple physical security controls prevent unauthorized access to University facilities. Cardholder data printed on paper or received by fax is be protected against unauthorized access. ECU owned merchant terminals are destroyed if no longer needed.

**h) Retention:** The merchant copy of receipts shall be kept for 3 years. Cardholder data must be deleted or destroyed before it is physically disposed (e.g. by shredding paper and shredding).

**i) Access Tracking:** All access to cardholder data is logged. Logs contain successful and unsuccessful login attempts and all access to the audit logs. Critical system clocks are synchronized with ECU’s time server, and logs include date and time stamps. Logs are secured, regularly backed up and retained for 6 months online and one year offline.

**j) Security Breaches – Incident Plan:** ECU adheres to all requirements pertaining to the establishment of a security incident plan as required by the PCI Data Security Standard and other applicable policies. This plan includes any actions necessary to secure any exposed data, to report the incident to appropriate university management, to report the incident to the Office of the State Controller, and adhering to applicable statues, including the NC Identity Theft Protection Act. Please reference OSC’s E-Commerce Policy entitled *Merchant Card Security Incident Plan.*

**SECP Merchant Cards Security Incident Plan**

### 9. Training

As specified by requirement number 12 of the PCI DSS, ECU requires all employees having access to merchant card data to review and sign its *PCI Security Awareness User Certification* statement annually. Please reference ECU’s certification statement: *PCI Security Awareness User Certification*. This document advises employees of the expectation of being aware of the sensitivity of data and of their responsibility for protecting the data.

Via ECU’s E-Commerce and PCI compliance Blackboard “class” the following documents will be made available as reference materials. All users will be “enrolled” in the class and reference is made to the State Controller’s SECP Website.

- a) SunTrust Merchant Services Operating Guide
- b) VISA Rules for Merchants
- c) Master Card Rules for Merchants
- d) PCI Data Security Standard

ECU’s E-Commerce Manager is responsible for training initiatives. Other training initiatives that are in progress and/or being considered include the following:

- a) Offering sessions at Financial Services Annual Training – usually in February;
- b) Training on Credit Card Balancing and Reconciliation using Clientline;
- c) Using Trustwave’s services for user training;
- d) Using the Cornerstone training program which includes a module on PCI.

Participation can be tracked using participant sign in sheets, and on-line attendance tracking as
10. Business Functions

Authorizations for merchant card payments are obtained as follows:

a) For face-to-face transactions, the card holder’s signature must be verified.

b) For on-line card not-present transactions using TouchNet, in general both Secure Code and Address Verification are required. There are a few merchants that have membership auto-renewals and in those instances only address verification is required.

c) Prior to the finalization of a merchant card transaction, an authorization approval code must be obtained from the merchant card processor – depending upon the capture method being used.

d) ECU prefers and primarily uses real-time authorizations; however, on occasion, telephone authorization is used.

e) If ECU cannot obtain authorization, the payment card is not accepted and an alternative means of payment will be requested.

f) If a suspected fraud is detected, code 10 authorization procedures as outlined in the SunTrust Merchant Services Operating Guide will be followed. Additional guidance for a Code 10 authorization is included in ECU’s Standard Operating Practice Code 10 Authorizations.

g) Reference is made to OSC’s E-Commerce Policy entitled, “Authorization for Merchant Card Transactions.”

Refunds and Credits for merchant card payments are processed as follows:

ECU does not issue cash refunds for payments made via payment cards. Total and/or partial refunds are issued based on the original transaction and to the card originally used.

ECU outsourced payment card processing for student tuition, fees, housing and dining charges to TouchNet and utilizes TouchNet’s PayPath for merchant card processing. Cashier's staffs are set up as reviewers and can only request refunds. The University Cashier and the Manager for Student Financial Services are set up as approvers and authorize the refund based on university records, reasons for the request, and supporting documentation provided by the cashier staff.

Fulfillment and Shipping of Goods: Currently ECU does not sell any items on line requiring item fulfillment and shipment of goods.

Cut-off Times and Close Outs are as follows:

The following cutoff times are established for POS terminal transactions: midnight daily; however, terminals can be closed manually as needed.

The following cutoff times are established for Internet transactions: 11:00 pm CST/12:00 midnight EST via TouchNet. The same timeframes apply for all other payment gateway processors.

All funds settle to the Credit Card Clearing Account specified in the Merchant Card Participant Setup Form. ECU has three credit card clearing accounts: Brody School of Medicine, School
of Dental Medicine and Main Campus.

11. **Fiscal Office Functions**

Reference is made to the guidelines specified on OSC’s SECP Website for [Merchant Card Reconciliation](#).

Merchant Card Receipts are accounted for daily and reconciled as follows:

Tools utilized in the reconciliation process include but are not limited to: DST’s Core Banking System, OSC’s Cash Management System (CMCS), MyClientLine, CPS-VCCT; and Wells Fargo’s CEO – Commercial Electronic Office.

The following reports are used in the reconciliation process: Treasury Reports from CEO, and ECU’s TYDF 100 Report, Sections 1-6, Summary Sheet for Certifications.

All merchant card payments are certified and reported through CMCS in accordance with established procedures, as “type 4” transactions on a daily basis.

The University Cashier’s Office, Financial Services and ECU Physicians are responsible for ensuring that all necessary reconciliations are performed.

Bank account statements received for the settlement account will be reconciled within 15 days of the statement being generated.

ECU has multiple merchant numbers associated with the MasterCard/VISA chain number and with the American Express chain number established for decentralized merchant processing within the various departments. To facilitate daily reconciliation and certification for all merchant activity, the University Cashier’s Office obtains Wells Fargo CEO treasury reports daily. All activity from each day’s settlement report is verified to receipts recorded in both the Banner Student and Miscellaneous Receipts modules. Discrepancies are investigated and resolved as identified. The University Cashier’s Office balancing reports are forwarded to Financial Services and state receipts are balanced daily to ensure a timely month end close.

**Chargebacks:** On occasion, cardholders originate payment disputes with their card issuers, resulting in chargebacks posting to the credit card clearing account.

Reference is made to OSC’s E-Commerce Policy entitled, “Customer Transaction Disputes” and to procedures prescribed in the [SunTrust Merchant Services Operating Guide](#).

Copies of transaction slips and other relevant documentation will be kept for a minimum of 18 months and in accordance with ECU’s official records retention schedule.

ECU will comply with requests from STMS and TouchNet for copies of transaction documents within the timeframe set forth in the notification/documentation request. ECU will act in good faith in resolving any disputes received from cardholders.
The credit card clearing accounts are set up as composite accounts to allow for debit chargeback entries. Allowing chargeback complies with merchant card requirements.

a) For student accounts, the amount of the chargeback is debited to the student’s account and a negative receipt adjustment is entered in the Banner system to reflect the cash reduction in the clearing account.

b) For all other transaction types, the University Cashier’s Office notifies the department where the credit card receipt originated that a charge has been reversed or charged back. The University Cashier’s Office requests the department prepare a negative receipt adjustment which is entered in the Banner system to reflect both the reduction in revenue and the reduction in the credit card clearing account.

Paying Invoices: All invoices for services received (e.g., SunTrust Merchant Services, CPS, etc) shall be paid timely, in accordance with established university procedures for accounts payable.

On a periodical basis, the interchange rates shall be inspected to ensure that the best rates are being obtained.

Responsibility for inspecting the invoices received and approving for payment is that of ECU’s Financial Services.

12. Other:

ECU complies with UNC FIT PCI compliance monitoring.

13. Signatures and Approvals:

The U.S. Federal ESIGN Act of 2000 gives the same legal protection to online signing as to traditional pen-and-paper signing.

Office of State Controller has a Master Services Agreement with DocuSign, Inc. that allows universities to participate in the contract.

ECU utilizes DocuSign for routing of documents and for the collection of signatures.

Approval Signatures collected through DocuSign’s routing process are original and official.

E-Signatures were affixed to this document via DocuSign as follows:

Dee Bowling, Director, Compliance Management, Financial Services, April 4, 2014
Robin Mayo, e Commerce Manager, April 4, 2014
Faye Steele, Specialist, Financial Services, April 9, 2014
Don Sweet, Chief Information Officer, April 11, 2014
Anne Jenkins, Associate Vice Chancellor for Financial Services, April 11, 2014
Frederick Niswander, Vice Chancellor for Administration and Finance, April 11, 2014
Amber Young, Central Compliance Manager, Office of State Controller, April 14, 2014