Current Status: *Active* **PolicyStat ID:** *6606714*

Origination:	*4/1/2011*
Effective:	*2/27/2015*
Last Revised:	*7/1/2011*
Owner:	*Alisa Schivley: Manager of Banking Operations*
Area:	*Business and Finance*

Debit/Credit Card Payment Policy; ICSUAM 6340.00

Policy Objective

It is the policy of the CSU that acceptance and processing of Debit/Credit Card payments adhere to prevailing rules, regulations, and laws pertinent to Debit/Credit Card payments processing. Each campus must prepare written procedures to implement this policy.

Policy Statement

The campus CFO or his/her designee must approve of all physical locations, websites, 3rd party processors, or any channel accepting credit card payments. Credit card payments will only be accepted at approved locations, using an approved CSU merchant card processor.

Cashiering sites accepting credit card payments should use only Point of Sale terminals or equipment supplied to the location by the campus' merchant card processor. All Point of Sale terminals and systems must be configured to prevent retention of the full magnetic strip, card validation code, PIN, or PIN Block cardholder data once a transaction has been authorized. If any account number, cardholder name, service code, or expiration date is retained, it must be encrypted and protected according to the standards outlined in the Payment Card Industry (PCI) Data Security Standards.

Manual requests to process a customer's credit or debit card must contain all of the following elements:

a. Properly signed/executed authorization from the cardholder (unless processing over the telephone as provided for in NACHA guidance on TEL transactions),

b. Credit/debit card account number with expiration date,

c. The card holder's correct billing address,

d. Authorization codes, if the cardholder is not physically present.

Should a manual initiating document be created in certain circumstances (via imprint or manual transcription of card information), such documents must be secured, and retained and/or disposed of according to the records retentions schedules.

All University deployed gateways must operate in conformity with prevailing PCI Data Security Standards (see Principles section below) and must be compatible with the University's merchant card processor.

Checks received and converted into an ACH transaction, or telephone authorizations for payment shall be processed in conformance to the National Automated Clearinghouse Association (NACHA) Operating Rules and compliant to relevant State and Federal rules and regulations (see Guidelines section below).

The University will not accept payment by email or fax transmission.

Benjamin F. Quillian
Executive Vice-Chancellor/Chief Financial Officer

Approved: February 4, 2011

Policy Operational Content

Applicability and Areas of Responsibility

Resources and Reference Materials

Useful Guidelines

POP Transactions

NACHA (National Automated Clearinghouse Association) has established rules to support a Standard Entry Class (SEC) transaction called the Point of Purchase (POP). In this service, a paper check is presented at the point of sale. The check is passed through an electronic check reader, which reads the Magnetic Ink Character Recognition (MICR) numbers at the bottom of the check [ABA routing and transit number, checking account number and check serial number]. The customer must sign the sales draft authorizing the electronic charge to his/her bank account. The check is then voided and returned to the customer with a copy of the sales draft receipt. The transaction is processed electronically and funds are withdrawn directly from the customer's checking account.

Subsection 3.8.1 of the National Automated Clearinghouse Association (NACHA) Operating Rules requires the following: For POP entries, the following may not be used as source documents: (1) checks drawn on corporate or business deposit accounts bearing auxiliary on-us numbers in the checking account number, (2) third-party checks, (3) credit card convenience checks, (4) obligations of a financial institution (e.g., traveler's cheques, cashier's checks, official checks, money orders, etc.), (5) checks drawn on the Treasury of the United States, a Federal Reserve Bank, or a Federal Home Loan Bank, (6) checks drawn on a state or local government, (7) checks payable in a medium other than United States currency or (8) eligible checks payable in excess of $25,000.

ARC Transactions

CSU departments processing consumer and small business checks as payment to open accounts receivable may elect to convert those checks to ACH debits in accordance with the Accounts Receivable Conversion (ARC) Standard Entry Class rules established by NACHA. Only consumer and small business checks are eligible for this treatment.

Consumer checks and business checks with no auxiliary on-us numbering in the checking account number and not exceeding $25,000 received by the CSU may be used to originate ACH debits to the consumer or small business bank account. The CSU electronically captures the check data (Account Number, Routing & Transit Number, Check Serial Number and Dollar Amount) and assembles the information into an ARC debit. The entry will flow from the CSU's bank to the consumer/small business bank and will be reported to the consumer/small business on his/her/its bank account statement as an electronically converted check. No prior approval for this conversion need be received from the consumer, however, prior notification to the consumer/small business, typically on the invoice, is required. Originators of ARC entries must also provide eligible payers with a method to opt out of the check conversion.

TEL Transactions

NACHA enacted the TEL Standard Entry Code (SEC) for telephone-initiated ACH items with the following steps:

1. TEL allows customers to authorize ACH payments to the CSU by a single telephone call. A standardized form should be developed and used by each CSU unit that allows payments to be effected by the TEL rules. These forms should be stored with extreme care and accessible only to persons with appropriate authorities. It is advisable to store the form digitally, encrypt the form and grant access only to authorized persons with id and password protection.
2. TEL eliminates requirements for signed or "similarly authenticated" customer pre-enrollment.
3. TEL permits recording of a customer's verbal authorization in lieu of confirmation mailings.
4. Through TEL, CSU units can now originate ACH debits as payment from any of their customers without requiring pre-enrollment.

NACHA rules require that a digital image of the check be retained in the event of a customer service inquiry or dispute. The consumer's bank may require a copy of the converted check at some future date. (See Appendix B for more information concerning Physical Security Guidelines)

Related Principles

PCI-DSS Standards Excerpted

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to data by business need-to-know 8. Assign a unique ID to each person with computer access 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

To receive a list and references to existing master contract(s) for the approved CSU merchant card processor(s) please contact the Chancellor's Office Contract Services & Procurement.

Sound Business Practices

Laws, State Codes, Regulations and Mandates

PCI DSS, Red flag rules, Reg E, Reg CC

Supersedes 3102.05

All revision dates:	7/1/2011, 4/1/2011

Attachments: