University of California
Business and Finance Bulletin

Office of the Executive Vice President
Business Operations
September 8, 2008

Number BUS-49	**Policy for Cash and Cash Equivalents Received** ***http://www.ucop.edu/ucophome/policies/bfb/bus49.html***	Refer all general questions to: Jerome.Frantz@ucop.edu Refer all campus questions to: Campus Controller

Business and Finance Bulletins Home Page: http://www.ucop.edu/ucophome/policies/bfb/

Table of Contents

I. REFERENCES

University of California

Accounting Manual chapter C-173, Cash: Cash Controls

Accounting Manual chapter C-173-61, Cash: Petty Cash Disbursements

Business and Finance Bulletin IS-3, Electronic Information Security

Business and Finance Bulletin RMP-4, Vital Records Protection:

Business and Finance Bulletin RMP-5a, Records Retention Program for Financial Documents Pertaining to Federal Awards to the University - References, Introduction, Records Destruction, Procedures, Responsibilities

Business and Finance Bulletin RMP-6, Microfilm Guidelines

Delegation of Authority-Revolving Fund Withdrawals, effective June 3, 2002

WEB ACH Primer guidelines, September 23, 2004

Guidelines for Accepting Credit Cards as a Form of Payment for Education, Registration or Other Fees, November 17, 2004

Internet Payment Gateway Guidelines for Payment Processing Model and Vendor Selection, June 30, 2002

Federal and State

Suspicious Activity Report: www.**fincen**.gov/**forms**/files/fin**109_sar**msb.pdf

California Civil Code §§1798.29 and 1798.82 (SB 1386, *Personal Information, Privacy*)

U.S. Secret Service *Know Your Money Guidelines*

Other Resources

NACHA (National Account Clearing House Association)

Payment Card Industry (PCI) Data Security Standards compliance requirements (www.pcisecuritystandards.org/index.htm)

II. INTRODUCTION

The University of California maintains financial policies that comply with state and federal law, and that incorporate recognized best practices for prudent oversight of the University's financial assets. This Bulletin establishes the University's policies related to handling and processing cash and cash equivalents, and defines roles and responsibilities related to receipt, safeguarding, reporting and recordkeeping for all University cash and cash equivalents. Its purpose is to ensure that these important University assets are protected, accurately and timely processed, and properly reported.

The University has established certain basic internal control principles applying to collecting and accounting for cash and cash equivalents.

A. Accountability

The campus is responsible for establishing procedures for cash and cash equivalents under that campus's control that identify:

1. Which individuals receive cash and cash equivalents and for what purpose
2. Where cash or cash equivalents are at all times; and
3. What transpired from the beginning to the conclusion of a cash handling process

Each individual who receives or has custody of University cash and cash equivalents must be held responsible for cash and cash equivalents under his or her control.

B. Separation of Duties

The Business Unit head is responsible for establishing procedures that ensure that no single individual is responsible for collection, handling, depositing and accounting for cash received by that unit. At least two qualified individuals must be assigned to carry out key duties of the cash handling process.

C. Physical Security and Data Transmission Security

The Business Unit head is responsible for establishing procedures that ensure that at all times:

1. Individuals who handle cash and cash equivalents are protected from physical harm.
2. Cash and cash equivalents in the custody of the unit are protected from loss.
3. Technology resources involved in processing cash and cash equivalents (i.e., hardware and confidential personal information) are protected from loss, corruption, or compromise to confidentiality.

D. Reconciliation of Accounts

The campus is responsible for establishing procedures to ensure that:

1. Cash and cash equivalents collected and reported as deposited are deposited to authorized University bank accounts in an accurate and timely manner.

2. General ledger recordings/transactions are accurate.

III. DEFINITIONS

For purposes of this Bulletin, terms are defined as follows.

A. Campus: a University campus, Medical Center, University-managed Department of Energy Laboratory ("Laboratory"), or other official University location.

B. Cash Handling Units (assignment of responsibility):

1. Main Cashiering Station
Campus operating unit from which collections are deposited directly to a University bank account.

2. Sub-cashiering Station
Campus operating unit from which collections are deposited to a Main Cashiering Station. These units typically perform cashier activities as a primary function and operate cash handling equipment.

3. Cash Handling Department
Campus operating unit that typically collects cash or cash equivalents and deposits to either a Main Cashiering Station or a Sub-cashiering Station.

C. When Types of Payments Received are Cash and Cash Equivalents[1].

1. Currency and Coin ("Cash")
Currency and coin are the most liquid of assets and must immediately and at all times be protected against loss.

2. Cash Equivalents (Money Orders, Travelers Checks, Cashiers Checks, Certified Checks)

a. Money Orders

Money Orders are financial instruments issued by a bank or other financial institution allowing the individual named on the order to receive a specified amount of cash on demand.

[1] Appendix A contains additional information defining each payment type.

b. Travelers Checks

Travelers Checks are preprinted, fixed-amount checks designed to allow the person signing to make an unconditional payment to someone else as a result of having paid the issuer (usually a bank) for that privilege.

c. Cashier's Checks (also known as Official Checks)

The term "cashier's check" means any check which:

- Is drawn on a depository institution;
- Is signed by an officer or employee of such depository institution; and
- Is a direct obligation of the depository institution

d. Certified Checks

The term "certified check" means any check certified by a depository institution as to

- The signature on the check being genuine; and
- The depository institution having set aside funds which:
  - (1) Are equal to the amount of the check; and
  - (2) Will be used only to pay that check

3. Checks

The term "check" means any negotiable demand draft drawn on or payable through an office of a depository institution located in the United States.

4. Automated Clearing House Payments (ACH)

ACH transactions are electronic payment instructions either to debit or credit a deposit account at a participating Receiving Depository Financial Institution ("RDFI").

5. Wire Transfers

Wire transfers are non-recourse, electronic fund transfers that move value from one bank account to another bank account through bookkeeping entries typically processed over the Federal Reserve Bank electronic network.

6. Credit and Debit Cards

Credit cards issued by commercial banks and financial institutions under the Visa and MasterCard brands and by independent companies (American Express and Discover) permit University clients to pay for services and goods by drawing against lines of credit granted by the card issuing companies.

Signature-based Debit Cards, also issued by financial institutions under the Visa and MasterCard brands, permit University clients to pay for services and goods by drawing against available funds resident in the payer's checking or savings account at the time of the payment.

PIN-based Debit Cards issued by financial institutions rely on connectivity to various debit card switching networks such as STAR, Interlink, NYCE, PULSE and several others. These cards permit University clients to pay for services and goods by drawing against available funds resident in the payer's checking or savings account at the time of the payment.

D. Petty Cash funds are those established for small expenditures that are not required to be processed under normal University purchasing procedures.

E. Change funds are those used to provide a constant amount of change, both in currency and coin, at cash collection stations.

IV. ROLES AND RESPONSIBILITIES

Policy IV.1: Campus administrators who have management responsibility for cash handling must assure that each individual who has or will have access to cash resources (including temporary, casual and student employees) has been appropriately vetted before access is granted. Background checks, demonstrated reliability in previous settings and evidence of cash-handling training are important factors in establishing an individual's qualifications. Each employee who handles and processes cash and cash equivalents must be bonded under the University self-insurance program upon assumption of cash-handling responsibilities. The University carries fidelity bonds (with high deductibles) to protect against losses associated with defalcation. These bonds provide coverage for all University employees effective as of the employee's hire date. There is no requirement to notify the bonding company when an individual's employment begins or ends.

The campus must perform background checks prior to employing cashiers, cash handlers and individuals in other critical positions. Each Business Officer is responsible for arranging the appropriate

background and employment checks in accordance with PPSM Policy 21 E., Appointment – Background Checks – Systemwide Guidelines on Designating Critical Positions. *

The hiring unit must seek an explanation for any reported felonies, misdemeanors, or judgments that were due to fraud related to cash, stocks, bonds or any other financial transactions before hiring or upon learning such information. Any individual with cash handling responsibilities must continuously maintain bondable status. If an employee with cash handling responsibilities is convicted of a crime, that conviction must be reported to the campus police department. If a cash handling employee loses the ability to be bonded, his or her cash handling responsibilities must be terminated.

A. Office of the President

1. The Vice President – Finance shall develop and publish University-wide cash handling policies and provide general coordination and assistance to campuses.

2. The Banking Services Group within UCOP Financial Management is responsible for managing all relationships with organizations that provide banking services to the University, opening bank accounts when requested by authorized campus employees, maintaining an inventory of authorized University bank accounts and conducting quarterly reviews of bank credit quality. See Section V, *Managing University Bank Accounts*, for additional information.

3. The Risk Management Group within UCOP Financial Management provides relevant and appropriate information to insurance carriers concerning University cashiering practices and procedures.

B. Campus/Laboratory Locations

1. Each Chancellor or Laboratory Director is responsible for establishing procedures to safeguard campus cash handling activities, including those of the Associated Students, in accordance with the policies established in this Bulletin. The Chancellor or Laboratory Director may delegate responsibility for oversight of all cash handling operations on the campus to a designated Cash Handling Coordinator.

2. Each Campus Controller or Laboratory Chief Financial Officer is responsible for implementing local procedures to comply with this Bulletin and for establishing criteria for granting all variances from these procedures when verifiable mitigating controls exist.

*minor change 8/25/2011

3. The Campus Cash Handling Coordinator is responsible for:

   a. Maintaining a liaison with the Campus Controller concerning cash handling matters

   b. Categorizing cash handling units and individuals performing functions related to cash handling accounting.

   c. Establishing local operating procedures in accordance with this Bulletin.

   d. Approving variances from this Bulletin as warranted by local circumstances.

   e. Reviewing and approving all proposed new or modified cash handling related applications, cash recording equipment, or methods of transporting cash.

   f. Performing an annual review of compliance with this Bulletin and informing the Campus Controller of risks associated with each campus cash-handling unit. Campus and Laboratory Police or their designee(s) must assist in all related security issues.

4. Revolving Fund Withdrawal Designee(s)

   The location shall designate in writing those individuals who are authorized to sign checks, drafts, or other orders for the payment of money or to approve/release electronic transfers of funds against University checking accounts. Any individuals so designated must be covered by a fidelity bond under the University self-insurance program.

5. Credit Card / Internet Payment Gateway Coordinator

   The Credit Card / Internet Payment Gateway Coordinator is an individual designated by the campus:

   a. As the central point of contact for the establishment of new credit card merchant accounts, with regard to set up with the merchant bank and internet service provider if applicable. Ensures that such accounts are properly instituted from the perspective of both vendor management and internal accounting standards.

   b. To maintain institutional records on “merchants” operating on campus, and to document equipment assigned to and services provided by each such merchant (merchant bank services and internet payment gateway services).

   c. To ensure that all University units processing credit or debit card transactions receive ongoing training regarding the data security requirements for handling cardholder data and that such units are complying with the credit card data security requirements for their operating environment including completion of mandated data

security questionnaires and system vulnerability scans if applicable.

d. To review credit card and internet payment gateway charges and qualification performance and to address problems with merchants as they arise to ensure the most cost-effective use of services.

V. MANAGING UNIVERSITY BANK ACCOUNTS

Policy V.1: Pursuant to Regents Standing Order 100.4 (pp) the President has the authority to open or make changes to official University bank accounts (see also Accounting Manual chapter C-173, Cash: Cash Controls).

Policy V.2: Only the Location Head (Chancellor or Laboratory Director) or an authorized designee may request approval from the President to establish a University bank account (see DA2130, Delegation of Authority-Revolving Fund Withdrawals).

Policy V.3: Any bank account opened for University purposes but not established and authorized by the Office of the President must immediately be reported for resolution to the Campus Controller and the Office of the President Banking Services Group.

Policy V.4: Accounts may be established only at financial institutions that meet minimum ratings published by major debt rating agencies. The Banking Services Group will perform a quarterly review of all depository banks at which the University maintains balances in excess of FDIC insurance amounts. Approved financial institutions must maintain an issuer rating on long term debt of A3 or higher as defined by Moody's Investor Service, A- or higher as defined by Standard & Poor's Corporation, or an Asset Peer Group rating of 65 or higher as defined by Sheshunoff Bank Rating Reports.

VI. OBTAINING APPROVAL TO ACCEPT CREDIT AND DEBIT CARD PAYMENTS

University units must seek approval to accept credit or debit cards in payment for goods or services. Upon approval, the unit is designated as a "Credit/Debit Card Merchant." Units must submit a cost benefit analysis to the campus Credit Card/Internet Payment Coordinator along with a request for permission to accept credit and/or debit cards as payment at the point of sale. Each campus must designate a Credit Card/Internet Payment Coordinator who has the authority to grant or deny a unit's request to accept credit or debit card payments. See: Guidelines for Accepting Credit Cards as a Form of Payment for Education, Registration or Other Fees

Policy VI.1: Each campus must develop implementing procedures regarding approval of credit and debit card merchants in compliance with this Bulletin.

The following facts must be considered when deliberating whether to approve a request for designation as a new campus Merchant:

1. Is the volume of transactions sufficient to justify the costs of offering payment by credit or debit card?
2. Which credit and debit cards (from which financial institutions) will be accepted?
3. Will the unit accept Visa, MasterCard, American Express or Discover Cards? Credit and/or debit cards?
4. Does the Unit have access to:
   i) a telephone line that will permit automatic credit and debit card processing by swiping the credit or debit card?
   ii) the internet for online payment processing options?
5. If the unit intends to accept *Cardholder Present* transactions, does the unit have a secure means of storing the signature verification provided by the buyer/payer at the point of sale or payment?
6. If the unit will accept *Cardholder Not Present* transactions, can it demonstrate excellent record-keeping practices and can it reassemble the transaction in the event of a dispute or a chargeback?
7. Is the unit able to demonstrate the ability to comply with Payment Card Industry Data Security Standards (PCI-DSS) requirements (www.pcisecuritystandards.org/index.htm)?
8. Have contracts for acquiring credit or debit card processing services been reviewed for appropriate terms, for representations that service providers will comply with PCI-DSS, and for assumption of liability for loss of any cardholder data while in the possession of the service provider.
9. Are procedures in place to protect personal, sensitive information from disclosures, including compliance with the state privacy standards[2] and similar regulatory requirements?
10. What procedures will be instituted to assure that payments are deposited directly into a University bank account, or if the funds will go to a third party, how long it will take for the funds to be deposited to an account generating interest for the University?

[2] California Civil Code §§1798.29 and 1798.82

Policy VI.2 University locations must use Merchant Card Processors approved under master University processing agreements. These agreements provide the most cost effectiveness and greatest level of service and compliance.

Policy VI.3 Any University unit wishing to process credit or debit cards must adhere to the PCI-DSS as it applies to the unit's processing environment. The classification of the environment will include such parameters as card present or card not present transactions, consideration of whether cardholder data is collected, transmitted, or stored on University systems, and whether such systems are accessible from the internet. Merchants are required to complete a questionnaire and make representations about the merchant's operating and data security practices. Depending upon the environment, the PCI DSS may require additional testing of merchant systems. Merchants must perform the tests indicated for their environment. A discussion of these security standards and additional testing requirements is included in Appendix-B Data Security. All units processing cards are required to review these standards annually and receive training annually on card security through their Credit Card / Internet Payment Gateway Coordinator.

Policy VI.4 Any University unit acquiring a payment application from a 3rd party vendor which will be operated on a University system and which will collect, store, or transmit cardholder data must only acquire such applications that are certified as complying with Payment Application Data Security Standards (PA-DSS, may also be referred to as PABP). While having a PA-DSS compliant application does not in and of itself ensure a merchant is PCI compliant, it will facilitate the process. Accordingly, any unit developing their own payment application that will operate on a University system should look to the PA-DSS standards for guidance on how to design the application so that it will not prevent the merchant from being PCI compliant.

VII. HANDLING CURRENCY, COIN & CHECKS

A. Currency and Coin

Currency and coin—or "cash"-- is the most liquid form of payment; that is, it is the most easily misappropriated. Cash must be protected against loss upon receipt and at all points thereafter. Physical security is the most important aspect of cash handling (see Physical Security, Section IX, for cash security best practices). It is important that cash handlers immediately establish a record of cash acceptance. To ensure employee accountability, managers must know *who* has authorized access to an asset, *why* he/she has access to the asset, *where* an asset is at all times, and *what* has occurred to the asset from beginning to the end of the cash-handling transaction cycle.

The following unique requirements are associated with cash.

Policy VIIA.1:

UC is exempt from reporting large cash transactions, because of its status as a governmental Entity (Internal Revenue Manual, Section 4.26.19.6(21). However, a University unit that observes a transaction or a series of transactions where both of the following occur:

a. The transaction or series of transactions involves funds or other assets of $2,000 or more, AND

b. The unit knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part) falls into one or more of the following categories:

- It involves funds derived from illegal activity, or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade any federal law or regulation, or to avoid any transaction reporting requirement under federal law or regulation; or
- Is designed to evade any regulations; or
- Has no business or apparent lawful purpose, or is not the sort in which the particular customer would normally be expected to engage, and the unit knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or
- Involves use of the money services business to facilitate criminal activity.

should contact their Campus police or the Banking Services Group and submit a SAR (FinCEN Form 109) no later than 30 calendar days after the date of the initial detection by the unit of facts that may constitute a basis for filing a SAR.

Policy VIIA.2: No University unit may accept non-U.S. currency as payment.

B. Checks, including Money Orders, Travelers Checks and Certified Checks[3]

The term "check" means any negotiable demand draft drawn on or payable through an office of a depository institution.

Policy VIIB.1: All checks must be made payable to the Regents of the University of California ("UC Regents"). Notices accompanying a request for payment should instruct payers

[3] See Appendix A for more details on these instruments

that checks will not be accepted if they are not properly made out to *UC Regents*. Checks should not be accepted if:

a. They are older than 180 days prior to the date of acceptance (unless a shorter time period is clearly marked on the face of the check) and no later than the date of acceptance

b. The payment amount is not readable, or the numerical amount does not match the written-out amount.

c. The check is signed by someone other than the holder of the account.

d. The check is stamped or otherwise identified as "Payable/Paid in Full" (if so, the check must be returned to the presenter, and must not be deposited).

Policy VIIB.4: Checks received and drawn on foreign bank accounts that are not acceptable at face value by the University's depository bank must not be recorded, but must be sent to the depository bank for collection.

VIII. PAYMENT CHANNELS – REQUIRED CONTROLS

This Section covers policies for receiving and recording cash and cash equivalents presented in person or through the mail.

A. General Cashiering Policies for Receiving and Recording Cash and Cash Equivalents

Policy VIIIA.1: Separation of duties must be maintained when cash is received. No single person should have complete control.

Policy VIIIA.1.1:

Cashiers shall not perform tasks incompatible with cashiering (e.g., collection follow-up of accounts receivable, distribution of payroll or other checks).

Policy VIIIA.1.2:

The person collecting cash, issuing cash receipts, and preparing the departmental deposit shall be someone other than the person performing the monthly review of the General Ledger or the person maintaining accounts receivable records.

Policy VIIIA.1.3:

Mailed remittances shall be verified and processed by two employees.

Policy VIIIA.2:
Individual accountability must be maintained and documented for all cash handling procedures:

Policy VIIIA.2.1:
Each cashier shall be assigned a unique identifier not accessible by or shared with other individuals. The unit must provide a cash register drawer, a cash drawer insert or another secure cash receptacle to which only the cashier has access. An individual endorsement stamp or its mechanical equivalent will be provided.

Policy VIIIA.2.2:
Cashiers must lock all cash in a drawer or secure receptacle whenever leaving the immediate area.

Policy VIIIA.2.3:
Documentation of cash differences must be maintained for each cashier.

Policy IXA.3: All cash transfers must be documented and the documentation of accountability maintained by category (i.e., currency, checks and other forms of payment).

B. Recording Cash and Cash Equivalents:

Policy VIIIB.1: Immediately upon receipt, checks must be restrictively endorsed "for deposit only".

Policy VIIIB.1.1:
Each Cashier must be provided an official endorsement stamp or its mechanical equivalent, identifying the cashier and department.

Policy VIIIB.2: An official University cash receipt shall be recorded for each collection. A copy of the receipt shall be provided to payers making an in-person payment and to payers making currency and coin payments through the mail. Although receipts shall be produced for check payments received through the mail, the mailing of a receipt to the payer is only required when the payer has requested a receipt.

Policy VIIIB.3: Under no circumstances will checks be routed to other offices to obtain recording information. When the proper account(s) to which a check should be credited cannot be readily determined, the check will be sent to the Main Cashier's Office. A "Cash Received Undistributed" recording will be made and a copy of

the check (in lieu of the check) will be distributed to appropriate offices for reference to determine the account distribution.

Policy VIIIB.4: Reductions of recorded cash accountability, e.g., voids and refunds, must be supported by all copies of the document involved, explained, and approved in writing by the cashier's supervisor at the time of occurrence where practical, but no later than the end of the day.

Policy VIIIB.5: A collection not recorded on cash register or point of sale equipment must be recorded on an official pre-numbered, multiple-part Cash Receipt.

Policy VIIIB.5.1:

The receipts must be used sequentially.

Policy VIIIB.5.2:

The form must include a statement that the form is recognized as a receipt only after validation by cashier's or cash handling employee's initials or signature, or by validation stamp to identify the cashier or cash handling employee recording the transaction.

Policy VIIIB.5.3:

All voided receipts must be retained (i.e., not given to the customer) and have signed approval by a supervisor.

Policy VIIIB.6: Electronic Based Cashier Point of Sale Equipment must meet the University security and operational standards, which are:

Policy VIIIB.6.1:

All cash registers and point of sale equipment must produce a cash receipt with campus identifier for each customer.

Policy VIIIB.6.2:

The equipment must have a feature for machine validation of cash-related documents.

Policy VIIIB.6.3:

The cash-recording equipment must be controlled by unique consecutive numbers generated automatically and recorded with each transaction, as well as imprinted on the customer receipt.

Policy VIIIB.6.4:

The numbering mechanism providing consecutive transaction number control must be accessible only to the manufacturer's service representative or appropriate personnel who are independent of that cashiering station.

Policy VIIIB.6.5:

Each cashier/remittance processor must be assigned a unique identifier that is not accessible to other individuals. A cash register drawer, cash drawer insert, and an endorsement stamp or its mechanical equivalent must also be provided.

Policy VIIIB.7: If a Remittance Processor is used, it must meet the security and operational procedures of the University which are:

Policy VIIIB.7.1:

The remittance system must provide a statement of activity, report, or electronic notification of activity to individual or department customers (i.e., post to student accounts).

Policy VIIIB.7.2:

The remittance system must have a numbering validation system that provides consecutive transaction number control that is accessible only to the manufacturer's service representative, or appropriate personnel independent of that cashiering station.

Policy VIIIB.7.3:

The remittance system must provide a unique identifier for each operator that is not accessible to others.

Policy VIIIB.7.4:

The remittance system must endorse checks and verify individual cashier transactions.

Policy VIIIB.7.5:

The remittance system must document all voided transactions.

Policy VIIIB.7.6:

The remittance system must have security in place so that previous day's transactions cannot be altered.

C. Point-of-Sale Equipment –Debit and Credit Card Processing

Policy VIIIC.1: Cashiering sites that accept MasterCard, Visa, American Express and/or Discover Card and PIN based Debit Card transactions will use only Point of Sale terminals or equipment supplied to the location by the campus' Merchant Card processor.

Policy VIIIC.2: 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 card holder 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.

D. Point of Purchase (POP) & Back Office Conversion (BOC) ACH Requirements.

Policy VIIID.1: A campus must comply with NACHA (National Automated Clearinghouse Association) rules that support Standard Entry Class (SEC) transactions called Point of Purchase (POP) and Back Office Conversion (BOC).

Point of Presentation/Payment

In POP, 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.

Back Office Conversion

In BOC, a paper check is presented at the point of sale and there must be written disclosure visible to the check writer at the point of sale advising the check writer that the check may be converted to an electronic ACH debit. The point of sale must provide the check writer with a means of opting out of the conversion of his/her check to an electronic ACH debit. Periodically or at the end of the business day, the retailer can then pass the check through an electronic check reader, which reads the Magnetic Ink Character Recognition numbers at the bottom of the check [ABA routing and transit number, checking account number and check serial number]. The check is then held for 14 calendar days after which

the check is to be destroyed. The transaction is processed electronically and funds are withdrawn directly from the customer's checking account.

The National Automated Clearinghouse Association (NACHA) Operating Rules require that only consumer checks and business checks, less than $25,000, with no auxiliary on-us code in the MICR line are eligible for this treatment. For POP and/or BOC entries, the following may not be used as source documents: (1) checks drawn on corporate or business deposit accounts, (2) third-party checks, (3) credit card checks, (4) obligations of a financial institution (e.g., traveler's checks, 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, or (7) checks payable in a medium other than United States currency.

E. Sale of Admission or Event Tickets

Policy VIIIE.1: Procedures for sales of admission or event tickets must meet the same standards and security requirements as those stated in the Cash/Cash Equivalent Receiving and Recording sections of this Bulletin (see Sections X and XI).

Policy VIIIE.2: Tickets must be consecutively pre-numbered or produced by electronic means when the numbering system is not accessible to ticket sellers. Each ticket is considered both the product and the receipt. All ticket sales must be balanced to their generated revenue on a daily basis. When admission tickets or individual items are sold at the gates of athletic or other events, cashiering equipment may not always be present, nor may receipts be issued. The campus department selling tickets or other items must develop adequate controls to safeguard tickets, including the use of pre-numbered ticket stock, and cash collections and to ensure that the number of tickets or items sold corresponds to the expected revenue from the sale of the tickets or items. These controls must be reviewed by the Cash Handling Coordinator and maintained for audit purposes.

Policy VIIIE.3: A full accounting of "tickets sold" against cash received and amount posted to the General Ledger should be completed periodically to make certain that assets distributed at the point of sale are properly converted to cash and that the cash is being deposited into the cashier's cash box.

F. Credit/Debit Card Batch Processing

Policy VIIIF.1: Mailed requests to charge a customer's credit or debit card must be processed as follows:

a) The authorization must be correctly executed/signed by the cardholder.

b) The credit or debit card account number must be provided in combination with the expiration date.

c) The authorization form must also include the correct billing address for the credit and/or debit card.

d) The card information received in the written authorization is then to be manually input into the Merchant Card processing equipment supplied by the Merchant Card processor. Authorized codes are to be noted clearly on the authorization form received from the customer.

e) All authorization forms that include customer account numbers and other personal information are to be stored with extreme care and accessible only to persons with appropriate authorities. Pursuant to card association rules, do not retain/store the card validation code beyond transaction authorization. If the card validation code is recorded on a form or collected by phone, that element must be destroyed once the transaction is authorized. PIN numbers for debit card transactions may never be gathered or entered for the customer. PIN debit transactions are only allowed in a card present environment where the customer enters the PIN directly into an approved keypad. If cardholder data must be maintained electronically, it must be encrypted with access restricted to authorized persons with ID and password protection (see the Payment Card Industry (PCI) Data Security Standards).

G. Accounts Receivable Conversion (ARC) - ACH Requirements

Policy VIIIG.1: A campus must comply with NACHA rules that support a Standard Entry Class (SEC) transaction called an Accounts Receivable Conversion (ARC). University units processing consumer 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. .

Consumer checks and eligible business checks received by the University may be used to originate ACH debits to a

consumer's or business's bank account. The University 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 University's bank to the consumer's or business's bank and will be reported on the account holder's bank statement as an electronically converted check. No prior approval for this conversion need be received from the consumer/business; however, prior notification to the consumer/business is required.

NACHA Operating Rules require that only those consumer checks and business checks less than $25,000 with no auxiliary on-us code in the MICR line are eligible for this treatment. For ARC entries, the following items may not be used as source documents: (1) checks drawn on corporate or business deposit accounts, (2) third-party checks, (3) credit card checks, (4) obligations of a financial institution (e.g., traveler's checks, cashier's checks, official checks, money orders, etc.), (5) checks drawn on the U.S. Treasury, a Federal Reserve Bank, or a Federal Home Loan Bank, (6) checks drawn on a state or local government account, or (7) checks payable in a medium other than U.S.currency.

H. Credit/Debit Card Telephone Transactions

1. Credit/Debit Card Processing

University units may accept credit and debit card payments requested by telephone. Such payments qualify for "cardholder not present" rules issued by the Credit Card Associations, under which the ultimate risk of fraudulent payment instructions resides with the Merchant (in this case, the University). The process is as follows:

Policy VIIIH.1.1: The correct billing address for the credit and/or debit card must be obtained.

The card information received by telephone authorization is then to be manually input into the Merchant Card processing equipment supplied by the Merchant Card processor. Authorization codes are to be noted clearly on the form used to document the data obtained from the customer.

Policy VIIIH.1.2: All data collection forms that include customer account numbers and other personal information should be

stored with extreme care and accessible only to persons with appropriate authority. Pursuant to card association rules, do not retain/store the card validation code beyond transaction authorization. If the card validation code is recorded on a form or collected by phone, that element must be destroyed once the transaction is authorized. PIN numbers for debit card transactions may never be gathered or entered for the customer. PIN debit transactions are only allowed in a card present environment where the customer enters the PIN directly into an approved keypad. If cardholder data must be maintained electronically, it must be encrypted with access restricted to authorized persons with ID and password protection (see the Payment Card Industry (PCI) Data Security Standards).

2. TEL ACH Requirements

Policy VIIIH.2.1: A campus must comply with NACHA rules that support a Standard Entry Class (SEC) transaction called the Telephone Conversion (TEL). NACHA enacted the TEL Standard Entry Code (SEC) for telephone-initiated ACH items with the following required steps:

a) TEL allows customers to authorize ACH payments to the University by a single telephone call. A standardized form should be developed and used by each University unit that allows payments to be initiated under the TEL rules. These forms should be stored with extreme care and accessible only to persons with appropriate authority. It is advisable to store the form digitally, encrypt the form and grant access only to authorized persons with id and password protection.

b) TEL eliminates requirements for signed or "similarly authenticated" customer pre-enrollment

c) TEL permits recording of a customer's verbal authorization in lieu of confirmation mailings, but one of these methods is required for all TEL transactions

Through TEL, University units can originate ACH debits as payment from any customer, without requiring pre-enrollment.

I. Prohibition on Payment with Credit/Debit Card Via Fax Transmissions

1. Credit/Debit Card Processing

Policy VIIII.1: Prohibition on Payment with Credit Card/Debit Card via Fax Transmission - The University should not accept payment instructions via fax transmission. This practice is prohibited as a violation of the intent of section 4(a) of the Uniform Commercial Code. The location Controller may grant variances provided appropriate compensating controls are in place. Under no circumstance may PIN debit transactions be processed by fax. PIN numbers should only be entered directly by the customer in a card present environment on an approved terminal. Any fax which includes PIN numbers must have the information removed and destroyed immediately without processing.

J. Payment with Credit-Debit Card Via the Internet

1. Information Security

Policy VIIIJ.1: Increasingly, the University will be accepting payments from customers over web-enabled connections facilitated by the Internet. The University subscribes to the Payment Card Industry (PCI) Data Security Standards.

Accordingly, when any University unit implements Web-based payment methods (whether operating the system internally or through a third party), the unit must comply with the following security standards (a more detailed description of the standards is provided on the PCI website and in the attached Appendix B – Data Security):

PCI Data Security Standard	
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

2. Credit/Debit Card Gateway

Policy VIIIJ.2.1: The University Banking Services Group in conjunction with campuses has developed guidelines concerning the use of Credit/Debit Card Gateways. All University deployed Gateways must operate in conformity with prevailing PCI Data Security Standards and must be compatible with the University's Merchant Card processor.

3. WEB ACH Transactions

Policy VIIIJ.3.1: University units may wish to deploy WEB ACH (aka e-checks) at their Internet Gateways to allow customers to pay for goods and services by authorizing an ACH debit to their bank accounts. Any University unit that deploys WEB ACH must use a University approved service provider. See the WEB ACH Guidelines published by the University Banking Services Group for more information on WEB ACH and e-checks.

IX. PHYSICAL SECURITY

Each campus should establish procedures to ensure physical security of cash at all times:

Policy IX.1: Excess cash must be removed from the cash register drawer during the business day and transferred to a secure cash handling area/vault. See Policy IX.6, below.

Policy IX.2: At the close of business, all cash must be secured as described in Policy IX.6, below.

Policy IX.3: Deposits must be adequately protected from loss while in transit. When necessary, armored car services (arranged through the Banking Services Group) or police protection (arranged through Campus Police) should be used.

Policy IX.4: Cash and cash equivalents must be locked in a secure receptacle or safe at all times except when signed out by a cashier for working cash.

Policy IX. 5: Each campus shall use lockable receptacles or burglarproof/fire resistant safes to store cash based on the following cash limits:

1. Up to $1,000 in a lockable receptacle
2. From $1,001 to $2,500 in a safe
3. From $2,501 to $25,000 in a steel-door safe, with a door thickness of not less than 1 inch and wall thickness of not less than ½ inch.
4. From $25,001 to $250,000 in a class TL-15 composite safe or better
5. Over $250,000 in a class TL-30 steel or better safe.

Deviation from these procedures may jeopardize the University's liability coverage.

Policy IX.6: If more than $2,500 in cash and securities is regularly on hand, the cash handling unit shall install a manual robbery alarm system must be installed for use during business hours to alert campus police (or the local police department for off site locations) if an irregularity occurs.

Policy IX.7: If more than $25,000 in cash and securities is stored, the cash handling unit must install an automated alarm system to alert campus police (or the local police department for off site locations) if the storage area is entered after business hours.

Policy IX.8: The safe's combination must be given only to supervisory and authorized personnel who must then commit the combination to memory. A record of the combination, sealed and opened only under double-custody to prevent undetected access, must be maintained away from the safe area.

Policy IX.9: A safe must be opened in such a way that other persons do not view the combination.

Policy IX.10: To the maximum extent practical, a safe must be locked between uses during business hours.

Policy IX.11: A safe's combination must be changed whenever a person who knows the combination leaves the employ of a cash handling unit. In addition, the combination must be changed at least once a year. Documentation must be maintained showing the date and the reason for the combination changes.

Policy IX.12: Each cashier must be provided with a separate lockable compartment in the safe to which only that cashier has access. Duplicate keys must be safely stored away from the safe and be retrieved only under dual control.

Policy IX.13: Funds or property not related to the operation of the University must not be stored in the safe/vault.

Policy IX.14: The Campus Cash Handling Coordinator, together with the Campus Risk Management and Police Departments, must review the physical setup of all cashiering stations to ensure that appropriate physical security is provided. As a general guideline, if a station collects more than $7,500 on a daily basis, the work area should be protected by doors and windows. All Main Cashiering Stations should record the handling and processing of cash and cash equivalents using surveillance cameras that capture actions in all areas of the Cashiering Station.

Policy IX.15: Campuses will develop and deliver cash handling training to all employees who handle cash. The training will include what to do in the event of a campus emergency. The training will be offered:

- When a new employee commences work in a cash handling job
- At least once per year for all cash handling employees to refresh knowledge concerning policies, procedures and techniques and to provide updated information on internal and external policies

Policy IX.16: Transporting deposits between cashiering sites or to the bank will be accomplished in a secure manner in order to protect the financial assets and individuals involved in transport.

Policy IX.17: Sub-Cashiering Stations and Cash Handing Departments will transport cash and cash equivalents to a Main Cashiering Station using the following methods:

- By secure armored car service
- By employees, in dual custody, transporting (walking or driving) the deposit to the Main Cashiering Station. If the deposit is in excess of $2,500, employees should be escorted by a Campus Security or Police Officer
- For endorsed checks and cash equivalents only, deposits may be put into the Campus Interoffice mail and sent to the Main Cashiering Station. The Depositing location should make copies of all checks and cash equivalents put into the Interoffice Mail in case the deposit is lost and needs to be reconstructed.

X. PREPARING DEPOSITS AND TRANSFERS TO BANKS

A. Accountability for and documentation of the custody of cash must be continually maintained when preparing and transferring deposits to banks.

Policy XA.1: Deposits must be validated and prepared under dual custody at all times in a safe and secure area.

Policy XA.2: The validation and preparation of cash deposits must not be visible outside of the deposit handling area.

Policy XA.3: A report of cash collections signed by the preparer must accompany each deposit to a Main Cashiering Station from a Cash Handling Department or Sub-Cashiering Station.

Policy XA.4: A night depository that satisfies the security standards in Section IX must be provided if cash transfers after business hours are necessary.

Policy XA.5: The Main Cashiering Station must record each deposit from a Cash Handling Department or Sub-Cashiering Station. All cash deposits must be counted under dual control. A receipt or its electronic equivalent for online department deposit systems must be forwarded to the Cash Handling Department or Sub-Cashiering Station no later than the next business day.

Policy XA.6: A report of cash recorded, cash deposited and cash collections that are over or short must be sent daily to the Accounting Office accompanied by supporting documentation (including cash register audit tapes, as applicable).

Policy XA.7: If electronic-mechanical or electronic cash registers are not in use, a report of account distribution of cash collections must also be sent daily to the Accounting Office.

B. Bank deposits must be made on a timely basis and supported with appropriate documentation.

Policy XB.1: Current day collections of Main Cashiering Stations must be deposited the same day, or at a minimum on the following business day.

Policy XB.2: Collections at Sub-cashiering Stations and Departments shall be deposited at the designated Main Cashiering Station at least weekly or whenever collections exceed $500.

Policy XB.3: All bank deposits must be accompanied by appropriate documentation, such as a numbered deposit slip.

XI. RECORDING TO THE GENERAL LEDGER

Policy XI.1: Deposits to banks must be reviewed, approved and recorded to the General Ledger in a timely manner and during the appropriate month

Policy XI.2: All journal entries must be reviewed and approved by designated employees in the Accounting Office. The preparer and reviewer/approver must be different persons.

Policy XI.3: Individuals with cash handling responsibilities may not prepare journal entries.

Policy XI.4: Processing incoming Wire Transfers and ACH Payments

- Wire Transfer and ACH credit transactions must be accessed through the bank's balance and transaction reporting system and recognized in the General Ledger each business day.
- Recording to the appropriate General Ledger and/or Receivable accounts must occur within two working days. All unidentified deposits will be posted to a specific "cash received undistributed" account.
- A unique identifier must be applied to the credits of an individual day's work, so the credits can be traced back to the correct deposit date. All funds received on a specific date must be applied in total for that date.
- A method of identifying and tracing funds in the specific "cash received undistributed account" must be in place.
- Separation of duties – the employee capturing and crediting the funds cannot also reconcile the bank statements.

XII. RETURNED ITEM PROCESSING

A. Cash Equivalents (non-coin & currency) and Checks

Cash equivalents may be returned unpaid by the banking system for a number of reasons but the primary cause of returned cash equivalents is counterfeiting or lost/stolen instruments which have been stop paid. Cash equivalents returned to the campus must be controlled during the process of attempting to collect on the returned amount. A non-cashiering unit is to provide oversight over the returned cash equivalent process.

Checks may be returned unpaid by the banking system for a number of reasons. The primary causes are insufficient funds, closed accounts and stop payment requests. Checks returned to the campus must be controlled during the process of attempting to collect on the returned amount. A non-cashiering unit should provide oversight over the returned check process.

Policy XIIA.1: Cash equivalents that are deemed to be uncollectible are to be returned by the depository bank to the designated non-cashiering unit.

Policy XIIA.2: Cash handlers must not be involved in the returned Cash Equivalent process.

Policy XIIA.3: The person who approves requests for write-off of uncollectible cash equivalents must not also maintain the inventory of returned cash equivalents.

Policy XIIA.4: A returned cash equivalent must be redeemed by a new payment.

Policy XIIA.5: The person maintaining the inventory of returned cash equivalents must not also handle the cash received to redeem returned cash equivalents.

Policy XIIA.6: No one person from the same office may perform more than one of the above functions (XIIA.2 - XIIA.5).

Policy XIIA.7: Physical security and accountability for returned cash equivalents must be maintained from the time of receipt of the returned item until final disposition

B. ACH Debit Transactions

ACH debits may be returned unpaid by the banking system for a number of reasons. The primary causes for returned debits are insufficient funds, non-sufficient funds, closed accounts, and lack of authorization or revocation of authorization. ACH debits returned to the campus must be controlled during the process of attempting to collect on the returned amount. A non-cashiering unit should provide oversight over the returned ACH debit process.

Policy XIIB.1: ACH debits that are deemed to be uncollectible are to be returned by the Originating Financial Depository Institution (depository bank) and communicated to the Accounting Department.

Policy XIIB.2: Cashiers must not be involved in the returned ACH debit process.

Policy XIIB.3: The person who approves the requests for write-off of uncollectible ACH debits must not also have physical access to the on-line ACH return functions.

Policy XIIB.4: A returned ACH debit must be redeemed by a new payment.

Policy XIIB.5: The person maintaining the inventory of returned ACH debits must not also handle the cash received to redeem a returned ACH debit.

Policy XIIB.6: No one person from the same office may perform more than one of the above functions (XIIB.2 - XIIB.5).

C. Credit/Debit Card Charge backs

Credit and debit card returns, also known as charge backs, are the consequence of:

1. Unauthorized/fraudulent use of a credit or debit card

2. An unresolved dispute between the payer and the University

   a. The payer argues that a good or service was not received

   b. The payer argues that a good or service was not received as promised (i.e. product or service failure)

   c. The payer argues that the Merchant (the University) overcharged for the good or service.

The campus will be notified that cardholder's (payer's) bank intends to process a chargeback to the Campus prior to the actual debit transaction. This "courtesy" is extended to all Merchants to permit the Merchant to "dispute" the chargeback, so these notifications should be researched and responded to upon receipt. Chargebacks are debited by the University's Merchant Card processor to the Campus Merchant Card Account. The chargeback will identify the Merchant ID (which translates to a specific campus business unit) that accepted the payment and that Merchant ID will be debited for the returned item. The Campus Credit Card Coordinator will notify the affected business unit of all chargebacks both during the courtesy notification period as well as when a chargeback is actually received.

Policy XIIC.1: Credit/Debit card chargebacks are to be returned by the Merchant Card processor to the designated non-cashiering unit.

Policy XIIC.2: Cashiers must not be involved in the returned Credit/Debit Card chargeback. Although they can be involved in defending the chargeback prior to the time it actually occurs.

Policy XIIC.3: The person who approves the requests for write-off of uncollectible Credit/Debit Card chargebacks must not maintain the inventory of returned Credit/Debit Card chargebacks.

Policy XIIC.4: A returned Credit/Debit Card chargeback must be redeemed by a new payment.

Policy XIIC.5: The person maintaining the inventory of returned Credit/Debit Card chargebacks must not handle the cash received to redeem returned Credit/Debit Card chargebacks.

Policy XIIC.6: No one person from the same office may perform more than one of the above functions (XIIC.2 - XIIC.5).

XIII. CONTRACTING WTH THIRD PARTIES TO PROCESS CASH AND CASH EQUIVALENTS (INCLUDING LOCKBOX SERVICES)

The University or an individual campus may need to engage a third party to assist in the processing and management of cash, cash equivalents and ACH transactions. Third parties may provide:

- Lockbox services
- Web/Internet interfaces to internal and external clients
- Processing of currency, coin and other cash equivalents
- Processing of electronic payments, particularly ACH entries
- Credit, Debit and Proprietary Card processing.

Relying on third parties to process University cash, cash equivalents and ACH transactions requires extreme care in the selection and ongoing management of such third parties. Accordingly, the following polices are necessary to safeguard University assets:

Policy XIII.1: The Banking Services Group must approve any third party relationship where the third party is in possession of University assets to process University cash, cash equivalents and/or ACH entries.

Policy XIII.2: Before a campus enters into any such relationship, the Banking Services Group must review of the third party's background, capabilities, financial condition and references.

Policy XIII.3: The Banking Services Group will at least annually review third-party relationships whereby the third party processes cash, cash equivalents and/or ACH transactions and actually has possession of University assets between $100,000 and $500,000 per year. The review will include an assessment of financial soundness and adequacy or services provided.

Policy XIII.4: Third parties that process cash, cash equivalents and/or ACH transactions and have possession of University assets in excess of $500,001 per year must be reviewed for financial soundness and adequacy by the Banking Services Group on at least a quarterly basis.

Policy XIII.5: Third parties that assist the University or individual campuses with management of cash and cash equivalents must enter into a University approved contract that requires at a minimum the same level of protection, regulatory compliance (including, but not limited to Payment Card Industry [PCI] Data Security Standards and State statutory or regulatory privacy requirements), insurance, bonding, and accurate/timely handling of cash, cash equivalents and/or ACH transactions and data as is established for the University itself by this Bulletin. The University is to be named as the sole loss-payee on any insurance and/or bonding agreements with third parties. All insurance carriers that provide protections to the University under third party agreements must be approved by Office of the President Risk Services.

For more information, see the Payment Card Industry Data Security Standards.

XIV. PETTY CASH AND CHANGE FUNDS

Policy XIV.1: Petty cash and change funds are provided as a service to operating units that require such operating funds. Campus policies must be established to appropriately protect these funds from loss.

For more information, see Accounting Manual chapter C-173-61

Policy XIV.2: Petty cash funds must be separately maintained from cashier change funds.

Policy XIV.3: Cash handlers must not exchange checks for currency to make change for each other. Any such change-making must be handled only by the custodian of the reserve change fund.

Policy XIV.4: An unannounced cash count and verification of change and petty cash funds for which cashiers and cash handling employees are accountable shall be performed on a periodic basis, at least quarterly, by someone other than the fund custodian. Verification of cash balances must be performed

in the presence of the petty cash/change funds custodian and must be documented. The Cash Handling Coordinator will approve the procedures. The results of the cash count are to be reported to the Central Accounting Office.

Credit and Debit Card Information

Cardholder Present: This is a sale/payment condition where the buyer/payer is physically on site with his/her credit or debit card available for "swiping" through the credit/debit card terminal made available to the business unit by University's Merchant Card processor. This transaction is completed when the buyer's/payer's credit/debit card issuer authorizes settlement of the transaction and the buyer/payer has signed the credit/debit card transaction receipt. It is the cash handling unit's obligation to check the authenticity of the signature by comparing the signature on the receipt to the signature on the back of the credit card. If the credit card has not been signed then, and only then, can the cash handling unit ask to see the buyer's/payer's driver's license.

The Cardholder Present model is beneficial to the University since it gives rise to the lowest discount rate from the Merchant Card Processor on the presumption that there will be lower rates of fraud and fewer chargebacks.

Cardholder Not Present: This is a sale/payment condition where the buyer/payer is not physically on site with his/her credit or debit card and, therefore, the cash handling unit has collected the cardholder data (card number, name, expiration date, billing address) by telephone, mail, or by Web site. This transaction is completed when the buyer/payer provides the needed information to the University via a telephone, or Web site and the University then presents that data to the Merchant Card processor which obtains an approval or rejection message from the buyer's/payer's credit card issuer.

The Cardholder Not Present model is efficient and allows transactions to be completed when the buyer/payer is not physically on site but it does gives rise to a higher discount rate from the Merchant Card Processor on the presumption that there will be higher rates of fraud and more chargebacks. Additionally, in most cases, the merchant site accepting payments in the Cardholder Not Present model typically must absorb any and all losses that arise from fraud or customer initiated chargebacks.

Detecting Counterfeit Money

The University has a role in maintaining the integrity of U.S. currency. You can help guard against the threat from counterfeiters by becoming more familiar with U.S. currency. Examine the money you receive closely. Compare a suspect note with a genuine note of the same denomination and series, paying attention to the quality of printing and paper. Look for differences, not similarities.

If you receive a counterfeit note:

- Do not return it to the passer.
- Write your initials and the date in the white border areas of the suspect note.

- Limit the handling of the note. Carefully place it in a protective covering, such as an envelope.
- Forward the note to a Main Cash Handling site or surrender the Currency or Coin only to a Campus police officer or a U.S. Secret Service Special Agent. If you work in a Main Cash Handling site, forward the note directly to the U.S. Secret Service. The U.S. Secret Service will normally mail the note back to you if it is not a counterfeit note or will send you a letter indicating that it is a counterfeit note.
- For more information on how to detect counterfeit money consult the U. S. Secret Service

Cash Equivalents (Money Orders, Travelers Checks, Cashiers Checks, Certified Checks)

Cash Equivalents, Money Orders; Travelers Checks; Cashiers Checks; and Certified Checks, are to be treated like all other checks (see "Checks" below.) Uniform Commercial Code (UCC) Sections 3 and 4 designate these Cash Equivalents as "Checks" and they are to be processed as any other Check. Cash Equivalents are to be made payable to "UC Regents."

Specific information you should know about Cash Equivalents:

1. Money Orders

   Money Orders are financial instruments issued by a bank or other financial institution allowing the individual named on the order to receive a specified amount of cash on demand. Often used by people who do not have checking accounts, a Money Order is a negotiable form of payment that is typically used by its purchaser to pay bills or other financial obligations or to purchase goods or services worldwide. A Money Order can be purchased at many supermarkets, financial institutions, or other independent retailers across the U.S. and at U.S. military installations. Immediately upon purchase of a Money Order the following information is to be completed:

   - The Pay to the order of line – all Money Orders presented to the University are to be issued payable to "UC Regents."
   - The signature and address of the purchaser or drawer of the Money Order
   - The date the Money Order was issued.

   Note: Money Orders are checks and are therefore subject to the stale dating rules of the Uniform Commercial Code. This means that Money Orders may be considered "stale" and therefore void at the conclusion of 180 days. However, this rule is seldom actually enforced; special care should be used in accepting Money Orders older than 180 days. In most State jurisdictions, non-negotiated Money Orders must be escheated to the State typically at the conclusion of year 2 or 3. Accordingly, Money Orders older than 2 years should not be accepted and the payer should be asked to acquire a new Money Order for payment of any University obligation. Alterations cannot be made to a completed Money Order including the "Pay to the Order Of" and the dollar amounts. Money orders may be purchased for any amount up to $1,000.

2. Travelers Checks

Travelers Checks are preprinted, fixed-amount checks designed to allow the person signing to make an unconditional payment to someone else as a result of having paid the issuer (usually a bank) for that privilege. Travelers Checks can usually be replaced if lost or stolen. Travelers Checks are generally considered "good as cash". Travelers Checks must be signed and made payable to the "UC Regents" in front of the cashier or the recipient when presented at any University point of sale or collection. Travelers Checks are available in different denominations and currencies. It is important to ensure that Travelers Checks accepted by any University point of sale or collection are payable **only** in U.S. dollars.

Note: Travelers Checks are subject to the same stale dating rules of the Uniform Commercial Code as are other checks. This means that a Travelers Check may be considered "stale" and therefore void after 180 days. While this rule is seldom actually enforced, special care should be used in accepting Travelers Checks older than 180 days. In most state jurisdictions, non-negotiated Travelers Checks must be escheated to the state typically at the conclusion of year 2 or 3. Accordingly, Travelers Checks older than 2 years should not be accepted and the payer should be asked to acquire a new Travelers Check for payment of any University obligation. Alterations cannot be made to a completed Travelers Check including the "Pay to the Order Of" and the dollar amounts.

3. Cashiers Checks (also known as Official Checks)

The term "Cashier's Check" means any check which:

- Is drawn on a depository institution;
- Is signed by an officer or employee of such depository institution; and
- Is a direct obligation of the depository institution.

A Cashiers Check is payable to a third party named by the customer who pays for the check at the time it is written. A Cashier's Check, which is drawn against the funds of the financial institution itself, differs from a Certified Check, which is drawn against the funds in a specific depositor's account. Cashiers Checks can be purchased for any amount. Cashiers Checks are suitable for times when a personal check is not acceptable, such as in real estate closings, apartment deposits, settlement of returned items or past due loans/debt, etc.

Note: Cashiers Checks are checks and are therefore subject to the stale dating rules of the Uniform Commercial Code. This means that a Cashiers Check may be considered "stale" and therefore void after 180 days. While this rule is seldom actually enforced, special care should be exercised in accepting Cashiers Checks older than 180 days. In most state jurisdictions, non-negotiated Cashiers Checks must be escheated to the state typically at the conclusion of year 2 or 3. Accordingly, Cashiers Checks older than 2 years should not be accepted and the payer should be asked to submit a new Cashiers Check for

payment of any University obligation. Alterations cannot be made to a completed Cashiers Check including the "Pay to the Order Of" and the dollar amounts.

4. Certified Check

The term "Certified Check" means any check with respect to which a depository institution certifies that:

- The signature on the check is genuine; and
- Such depository institution has set aside funds which:

  (i) Are equal to the amount of the check; and

  (ii) Will be used only to pay such check

A Certified Check is a check a bank has "certified" as having enough money in the maker's account to cover the amount of the check. The bank sets funds aside so that even if other checks were drawn upon a particular account, the check will remain good. Like Cashier's Checks, Certified Checks are immediately good upon presentation since the bank guarantees the funds and the recipient does not have to wait until the check "clears."

Note: It is not uncommon for individuals or businesses to stamp or write the word "Certified" on the front of a check. Unless the check is officially certified by the financial institution that holds the account on which the check is payable, the word "Certified" has no meaning. Use reasonable care when accepting Certified Checks.

Automated Clearing House Payments (ACH)

The Operating Rules of the National Automated Clearinghouse Association (NACHA) govern ACH transactions. ACH transactions are payment instructions to either debit or credit a deposit account at a participating depository financial institution. An ACH transaction is a batch-processed, value-dated electronic funds transfer between originating (ODFI) and receiving (RDFI) depository financial institutions. ACH payments can either be credits, originated by the accountholder sending funds (payer), or debits, originated by the accountholder receiving funds (payee).

ACH transactions are sent in batches to ACH operators for processing one or two business days before settlement dates. The ACH operators deliver the transactions to the receiving institutions at defined times. There are two national ACH operators. The Electronic Payments Network (EPN) is a private processor with approximately 30 percent of the national market. The Federal Reserve Banks process the remaining share of the market.

In all ACH transactions, instructions flow from an ODFI to a RDFI. An ODFI may request or deliver funds and transaction instructions and funds are linked using codes for record keeping. If the ODFI sends funds, it is a credit transaction. Examples of credit payment transactions include financial aid and other refunds, payroll direct deposit, Social Security payments, and dividend and interest payments. Corporate payments to contractors, vendors, or other third parties are also

common ACH credit transactions. If the ODFI requests funds, it is a debit transaction and funds flow in the opposite direction. Examples include online check payment transactions, check conversion via POP, BOC or ARC, collection of insurance premiums, mortgage and loan payments, consumer bill payments, and corporate cash concentration transactions.

Financial institutions originating customer payments have a binding commitment for payment to the ACH operator when the ACH files are distributed. Settlement for Federal Reserve Bank ACH credit transactions is final at 8:30 a.m. Eastern Time (ET) on the settlement day, when posted to depository financial institution accounts. Settlement is final for ACH debit transactions when posted at 11:00 a.m. ET on the settlement day.

Credits Received (Home Banking Payments)

Third parties, both financial institutions and Business Service Processors (BSPs[4]), accept and process "bill payment" instructions. Therefore, University clients may use these systems to make payments on "open accounts." It is possible that a Campus will receive a check with a log of payments being made by that check. It is also possible that the Campus will receive an ACH credit that includes one or more payments. The financial institution or BSP will typically provide the Campus with a paper or electronic record of the payments settled by the ACH credit.

1. Debits Originated by the University

   The University will be asked by clients or authorized by NACHA Operating Rules to debit client bank accounts as payment for goods or services. In each instance, the payer must give its authorization to the University to debit its account (in the case of the ARC, NACHA rules presume that receipt of a paper check translates into the needed authority to debit the consumer payer's account through the ACH).

   NACHA has established specific payment types (transaction codes) for each interaction with the client summarized below:

WEB	Internet originated ACH debit to a client's account
TEL	Telephone originated ACH debit to a client's account
POP	Point of Purchase originated ACH debit to a client's account
BOC	Back Office Conversion
ARC	Conversion of an Account Receivable payment received as a check to an ACH debit to a client's account. ARC is presently only authorized for conversion of consumer checks or business checks with no Auxiliary on-us field less than $25,000. All other checks are not eligible for ARC treatment
PPD	Prearranged, preauthorized ACH debit to a client's account.

[4] Key BSPs are firms such as CheckFree, Metavante, e-Princeton, etc.

Automated Remittance Processing

University units may elect to operate either directly or through third party processors, automated remittance processing services (otherwise known as lockboxes). To be fully effective, the following key functions are to be included in any such service:

1. A unique post office box address is to be used for the receipt of lockbox remittance.
2. The lockbox operator should pick up all incoming mail each morning and deliver it to the lockbox operating site for processing in order to meet check clearing deadlines established by the depository bank
3. The contents of remittance envelopes should be removed from and examined carefully to certify that the checks are made payable to an acceptable payee (Regents, University, etc.), are dated correctly, are signed and are made out for the correct amount. All checks should be reviewed carefully to assure that no restrictive notations such as "paid in full" are visible on the check
4. Checks are to be copied (digital is preferred) and stored for research and customer service purposes.
5. Envelopes and other remittance documents may also be retained either in hard-copy or digitally for possible future use.
6. The lockbox should create batches of checks for deposit in accordance with instructions set forth by the depository bank.

    a. The full deposit of checks should be made to the depository bank on time in order to achieve the greatest availability of funds.

    b. All data stored from the lockbox should be safely kept in accordance with University data retention standards.

Reason Codes for Return of Payments, by Type

The following chart highlights the primary reasons for return of each of the payment types in the left hand column. For instance, every payment type except ACH may be returned to the depositor if the entry was deemed to be counterfeit.

	Counterfeit/ Altered Item	Non-Sufficient Funds	Stop Paid	Stale Dated	Account Closed	Fraudulent Endorsement	Not-Authorized	Product or Service Dispute
Cash	X							
Cash Equivalents	X		X	X		X		
Checks	X	X	X	X	X	X		
ACH		X			X		X	
Credit/ Debit Cards	X						X	X

Time Limits by which Payment Types Must Legally Be Returned

	Counterfeit	Non-Sufficient Funds	Stop Paid	Stale Dated	Account Closed	Fraudulent Endorsement	Not-Authorized	Product or Service Dispute
Cash	Days							
Cash Equivalents	24 hour reclamation		24 hour reclamation	24 hour reclamation		90 days		
Checks	24 hour reclamation	24 hour reclamation	24 hour reclamation	24 hour reclamation	24 hour reclamation	90 days		
ACH		24 hour reclamation			24 hour reclamation		60 days	
Credit/ Debit Cards	60 days						60 days	60 days

APPENDIX B

DATA SECURITY

Protection of University assets and technology resources that support the University enterprise is critical to the functioning of the University. University information assets are at risk from employee error, malicious or criminal action, system failure, natural disasters, etc. Such events might result in damage to or loss of information resources, corruption or loss of data integrity, interruption of the activities of the University, or compromise to confidentiality or privacy of members of the University community.

University cashiering functions routinely process highly sensitive data both in paper and electronic form. Accordingly, it is critical that all cashiering locations process and store sensitive data with utmost care to protect the privacy of University constituencies and to avoid any financial losses that may arise from the unauthorized use or disclosure of confidential information.

The University has issued data retention and security polices for both electronic and paper media. Accordingly, this Bulletin refers each University Cashiering site to the following policy statements for general guidance concerning the receipt, handling, storage and retention of private, restricted data:

Electronic Information Security is guided by Business and Finance Bulletin IS-3.

Any credit or debit card cardholder information collected, stored, or transmitted as part of a card transaction is further regulated under the Payment Card Industry (PCI) Data Security Standards. Compliance with these standards is mandatory for all University units accepting credit/debit cards for payment. Failure to comply can result in significant fines and loss of the ability to process such transactions. University units processing card transactions must understand the data security rules applicable to their processing environment. The Credit Card / Internet Payment Gateway Coordinator assists in that training as part of authorizing the unit to process cards (see Policy VI.1).

Physical Records Security (including microfilm) is guided by Business and Finance Bulletins RMP-4, Vital Record Protection, RMP-5a, Records Retention Program for Financial Documents Pertaining to Financial Awards to the University and RMP6, Microfilm Guidelines.

Refer to Senate Bill 1386 for privacy requirements.

Specific Data Security guidelines for University Cashiering sites:

1. The privacy and confidentiality of all accessible data is to be maintained and it is understood that unauthorized disclosure of personal/confidential information is an invasion of privacy, may be illegal, and may result in disciplinary, civil and/or criminal actions against an individual.

2. Training in data security must be provided by each campus to any user of highly secure information, especially private information, related to management, use, and protection. This training may be overarching or specific (such as FERPA training for student data).

3. Systems should not include restricted[5] information unless absolutely necessary.

4. Restricted data elements (e.g., Social Security Number, ethnicity, date of birth and financial information such as credit card number or bank account number) should never be used as the 'key' to a system.

5. The University subscribes to the Payment Card Industry (PCI) Data Security Standards. Refer to Policy VIIIJ.1for further detail on these standards. While many of the standards are similar to other data security practices in this Appendix, there are some unique requirements which card processing units must become familiar with.

6. Central to any data security program is testing. Any University unit processing credit or debit card transactions and storing such data electronically or transmitting such data over the internet using University systems must perform a detailed review of the Payment Card Industry (PCI) Data Security Standards with their IT support staff to ensure they can comply with all requirements for data protection applicable to their processing environment. Based on the environment, these merchants may be required to perform some or all of the following, to ensure they are secure:

    - Subscribe to a service to regularly scan such systems for vulnerability by a vendor authorized by the Payment Card Industry to perform such services;
    - Test systems regularly as outlined in the PCI Data Security Standards with a wireless analyzer to detect any wireless access, in particular, any unauthorized wireless access;
    - Utilize intrusion detection systems as outlined in the PCI Data Security Standards;
    - Test systems annually as outlined in the PCI Data Security Standards using network layer and application layer penetration tests;
    - Complete an annual data security questionnaire provided by the Payment Card Industry which is tailored to their operating environment (see the Payment Card Industry (PCI) Data Security Standards for the questionnaires and descriptions of the processing environments to which they apply).

7. Do not download restricted data from a database system to your laptop or desktop unless there is an unavoidable business need. If this information is downloaded, ensure that it is protected against hacking or loss (e.g., at a minimum by encryption), and that it is removed as soon as possible.

8. Do not e-mail restricted data, either in the body of an e-mail or as an attachment.

9. Encrypt stored restricted data. Protect the encryption key from unauthorized disclosure.

10. Credit card account and transaction information must not be sent via unencrypted e-mail messages over the Internet.

[5] See BFB IS-3 for a definition of Restricted Data

11. Use strong cryptography and security protocols to protect sensitive credit card data during transmission over the internet. The Payment Card Industry Data Security Standards spell out the current requirements which may include such methods as: Secure Sockets Layer (SSL)/Transport Layer Security (TLS) and Internet Protocol Security (IPSEC).

12. Never store payment data on a web server or cache anywhere in memory related to a web server. Payment data may only be stored in a separate, secure database with appropriate firewalls to prevent unauthorized access. Anti-virus software must be deployed on all systems commonly affected by viruses.

13. Ensure that critical data is backed up and that a business resumption plan exists and that backed up data is stored in a secure manner.

14. Any paper records with full credit or debit card numbers must be only accessible by authorized personnel, kept locked up when not in use, and destroyed (cross-cut shredding or pulping) when no longer needed.

15. Customer receipts may display no more than the last 4 digits of any credit or debit card number and no expiration date may be displayed. Best practice for merchant receipts, reports, and systems is to similarly display no more than the last 4 digits of any credit or debit card number. Merchant receipts must also suppress the expiration date. While the PCI-DSS rules allow merchant system inquiries and reports to display the 6 leading digits and the last 4 digits of any card number, merchants are strongly advised to limit such displays to the last 4 digits only.

    Customer receipts and reports maximum display: XXXX XXXX XXXX 1234

    Highly recommended system display: XXXX XXXX XXXX 1234

    Allowed system display, but discouraged: 1234 56XX XXXX 1234

16. When processing credit or debit card transactions, the card validation code (security code on the card), the PIN, and the PIN Block from the card must never be retained beyond the need to authorize a transaction. Similarly, any card present system electronically reading the magnetic strip on a card must be programmed not to retain the magnetic strip data once the transaction has been authorized. This includes any data logging systems.

17. All contracts used to acquire card processing services from a 3rd party must specifically state the processor is/will be PCI DSS compliant, the processor will provide regular evidence of certification, and that the processor will assume responsibility (liability) for the security of any such cardholder data in its possession. All contracts used to acquire payment applications which will operate on University systems and collect, transmit, or store cardholder data must be Payment Application Data Security Standard certified (PA-DSS, may also be referred to as PABP).

18. Any suspected loss of unencrypted restricted data must be reported in accordance with IS-3.

System and Data Access

1. Access to the system should be given only to individuals when it is necessary to perform their job duties, and the process owner should approve any access granted.
2. Restrict physical access to student payment and personal data.
3. Restrict physical entry to e-commerce web servers to authorized personnel.
4. An individual's access should immediately be revoked when his/her job duties no longer require that access. A list of individuals with systems access should be reviewed at least annually by the process owner to ensure that only authorized individuals have access.
5. Assign a unique ID to each person with computer access to payment data.
6. Maintain the ability to track employee access to payment data through use of unique IDs.
7. Do not share passwords. Restrict access to information based on a need to know basis. Lock your computer when not in use. Set-up computers to time out and require users to sign in when the computer is not used within a reasonable amount of time. When you print restricted documents, pick them up immediately and shred when finished.
8. Change employee passwords regularly.