

# **California State University**

## **CASHIERING POLICY**

**May 18, 2009**

# Cashiering Policies of the California State University

Owner: Sean Boylan, CO Resource Management

The following cashiering policies are also applicable to operation of a CSU Auxiliary Organization in the handling of state funds on behalf of and/or under contract with the CSU.

## POLICY FOR CASH AND CASH EQUIVALENTS RECEIVED

### Table of Contents

	<u>Page</u>
I. <a href="#">References</a>	3
II. <a href="#">Introduction</a>	4
A. Key Objectives	4
1. Accountability	4
2. Separation of Duties	4
3. Security (Physical and Information)	4
4. Reconciliation of Accounts	5
III. <a href="#">Definitions</a>	5
IV. <a href="#">Roles and Responsibilities</a>	8
A. California State University Chancellor's Office	8
B. Campus Administration	8
V. <a href="#">Conditions for Employment in a Cash Handling Environment</a>	10
VI. <a href="#">Managing California State University Bank Accounts</a>	11
VII. <a href="#">Establishing Credit and Debit Card Merchants</a>	11
VIII. <a href="#">Payment Types</a>	13
A. Currency and Coin	13
B. Checks	14
IX. <a href="#">Payment Channels</a>	14

A.	General Cashiering Policies for Receiving and Recording Cash and Cash Equivalents	14
B.	Cash Receiving and Recording	15
C.	Point of Sale Equipment - Debt and Credit Card Processing	18
D.	Point of Purchase ACH Requirement	18
E.	Sale of Admission or Event Tickets	19
F.	Credit/Debit Card Batch Processing	20
G.	Accounts Receivable Conversion ACH Requirements	20
H.	Telephone	21
I.	Fax	22
J.	Internet	22
X.	<a href="#"><u>Physical Security</u></a>	24
XI.	<a href="#"><u>Preparing Transfers and Deposits to Banks</u></a>	26
XII.	<a href="#"><u>Recording to the General Ledger</u></a>	27
XIII.	<a href="#"><u>Returned Item Processing</u></a>	28
A.	Cash Equivalents and Checks	28
B.	ACH Debits	29
C.	Credit/Debit Card Chargebacks	30
XIV.	<a href="#"><u>Third Party Relationships (includes Lockbox)</u></a>	31
XV	<a href="#"><u>Petty Cash and Change Funds</u></a>	32
Appendix A:	<a href="#"><u>General Information</u></a>	33
Appendix B:	<a href="#"><u>Data Security</u></a>	40

I. REFERENCES

Internal Revenue Service [Form 8300](#), Report of Cash Payments over \$10,000 Received in a Trade or Business

Internal Revenue Service [Publication 1544](#), Reporting Cash Payments of over \$10,000

Purchase Card Industry (PCI) Data Security Standards compliance requirements.  
See:

[http://usa.visa.com/download/business/accepting\\_visa/ops\\_risk\\_management/cisp\\_PCI\\_Data\\_Security\\_Standard.pdf?it=il/business/accepting\\_visa/ops\\_risk\\_management/cisp.html|PCI\\_Data%Security%Standard](http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf?it=il/business/accepting_visa/ops_risk_management/cisp.html|PCI_Data%Security%Standard)

State of California Information Practice Act ([Senate Bill 1386](#)), Peace. Personal information: Privacy

The [United States Secret Service](#)

## II. INTRODUCTION

This document establishes the California State University's ("CSU") policies and procedures related to handling and processing cash and cash equivalents. Its purpose is to ensure that these important CSU assets are protected, accurately processed, and properly reported.

Policy statements are specifically identified and numbered as Policies in this document. Procedural statements are included, but do not have specific numbers. **All policy statements are indicated in bold type.**

Certain basic internal control principles must be adhered to in regards to collecting and accounting for cash and cash equivalents. These basic principles are articulated below:

### A. Key Objectives of this document:

#### 1. Accountability

- Ensures that CSU employees who process and/or handle cash and cash equivalents can be held responsible in fulfilling their duties.
- Accountability is present when the following three (3) areas are addressed:
  - a) Knowledge of who has or had access to, and why he/she has or had access to, cash and cash equivalents;
  - b) Knowledge of where cash or cash equivalent assets are at all times; and
  - c) Knowledge of what transpired from the beginning of a cash handling process to the conclusion of the process.

#### 2. Separation of Duties

- Ensures that two (2) or more qualified and authorized persons are involved in the key, most sensitive activities related to the collection, handling, depositing, and accounting processes.

#### 3. Security (Physical and Information)

- Ensures that employees involved in the handling of cash and cash equivalents are, at all times, protected from physical harm.

- Ensure that cash and cash equivalents are, at all times, protected from loss or misuse.
  - Ensure that technology resources (i.e. hardware and confidential payment information) are, at all times, protected from loss, corruption or compromise to confidentiality.
4. Reconciliation of Accounts
- Provides assurance that cash and cash equivalents collected and reported as deposited are deposited accurately and timely into authorized CSU bank accounts.
  - Provides assurance that general ledger recordings/transactions are accurate.

### III. DEFINITIONS

For purposes of this document:

- A. The term “Campus” is defined as a CSU Campus or other official CSU location.
- B. Cash Handling Units are defined generally as follows for assignment of responsibility):
1. Main Cashiering Station  
Campus operating unit from which collections are deposited directly to a CSU bank account.
  2. Satellite Cashiering Station  
Campus operating unit from which collections are deposited to a Main Cashiering Station. These units typically perform cashiering activities as a primary function and operate cash handling equipment. Satellite Cashiering Stations may deposit directly to approved depository bank accounts on behalf of Main Cashiering Stations.
  3. Cash Handling Department  
Campus operating unit that typically collects cash or cash equivalents and deposits to either a Main Cashiering Station or a Satellite Cashiering Station.

C. Types of Payments Received -- Cash and Cash Equivalents:

Additional information defining each payment type can be found in Appendix A of this document.

1. Currency and Coin (“Cash”)  
Currency and Coin are the most liquid of assets and must be immediately, and at all times, protected against loss or misuse.
2. Cash Equivalents (Money Orders, Travelers Cheques, 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.

b. Travelers Cheques

Travelers Cheques 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. Cashiers Check (also known as Official Check)

The term “Cashier’s Check” means any check which is:

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

**d. Certified Check**

The term “Certified Check” means any check for which a depository institution certifies that:

3. (2)
  - The signature on the check is genuine; and
  - Such depository institution has set aside funds which:
    - (1) Are equal to the amount of the check; and
    - (2) Will be used only to pay such check.Checks

The term “check” (including those instruments issued and commonly called warrants by the State of California) means any negotiable demand draft drawn on or payable through a United States office of a depository institution that is a qualified member of the United States’ Federal Reserve Bank.

4. Automated Clearing House Payments (ACH)

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

5. Wire Transfers

Wire Transfers are non-recourse, electronic funds transfers moving value from one bank account to another bank account through bookkeeping entries typically processed over the United States’ Federal Reserve Bank’s 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 CSU clients to pay for services and goods by drawing against lines of credit granted by the card issuing banks/companies.

Signature-based Debit Cards, also issued by financial institutions under the Visa and MasterCard brands, permit CSU 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, also 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 CSU 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 established for small expenditures when the use of regular purchasing procedures is not required.
- E. Change Funds are used to provide a constant amount of change, both in currency and coin, at cash collection stations.

#### IV. ROLES AND RESPONSIBILITIES

##### A. CSU Office of the Chancellor

1. The Chief Financial Officer (CFO) shall develop and publish CSU-wide cash handling policies and procedures and provide general coordination and assistance to Campuses. The CFO shall:
  - a. Select the commercial banks into which funds of the CSU are deposited and from which such funds are disbursed,
  - b. Designate the name of the CSU to all bank accounts and assume direct ownership of such bank accounts, including time certificates of deposit, and to make withdrawals from or close such accounts,
  - c. Designate representatives of the CSU who may sign checks or other orders for the payment of money, including electronic transfers of funds (EFT), Credit/Debit cards, wire transfers and ACH transfers, and to approve the use of and direct banks to honor facsimile signatures,
  - d. Make arrangements for internet payment services, lockbox, electronic transfer of funds, escrow services, credit/debit card and other services to facilitate the collection or disbursement of funds, and
  - e. Open, make changes to, and close CSU bank accounts.

These duties may be further delegated by the CFO to the Assistant Vice Chancellor-Financial Services and the Senior Director-Financing & Treasury or other Chancellor's Office representatives, as appropriate.

2. Cash Management Operations ("CMO"), a unit of the CSU Office of the Chancellor, is responsible for managing all relationships with organizations that provide banking and/or payment services to the CSU, opening, changing instruction to, and closing bank accounts when requested by authorized Campus employees and authorized by the CFO or his/her delegates, maintaining an inventory of authorized CSU bank accounts and conducting periodic reviews of bank credit quality. See section VI, Managing CSU Bank Accounts, for additional information.
3. Cash Management Operations must approve the use of any Third Party that is in possession of CSU assets to process CSU Cash, Cash Equivalents, Checks and/or ACH entries.

B. Campus Administration:

1. Each Campus President is responsible for all Campus cash handling activities in accordance with the policies and procedures established in this document. The Campus President is also responsible for making requests to the CFO and his/her delegates to open, make changes to, or close bank accounts. The President may delegate the responsibility for all cash handling operations on the Campus to the Campus Chief Financial Officer (Campus CFO).
2. The Campus CFO may delegate to the Associate Vice President and/or Controller responsibility for implementing this policy on a Campus level and managing the process for granting all variances from these procedures when warranted by local circumstances.
3. The Associate Vice President and/or Controller, who may create and delegate appropriate authorities to the Cash Handling Coordinator, should accept responsibility for the following:
  - a. Categorizing cash handling departments and individuals performing functions related to cash handling accounting.
  - b. Arranging for the preparation and implementation of operating procedures in accordance with this document.
  - c. Approving and documenting variances from these policies and procedures when warranted by local circumstances.
4. Cash Handling Coordinator, when created by and delegated authorities by the Associate Vice President and/or Controller, should accept responsibility for the following:
  - a. Serving as the central point of contact for implementing these policies and appropriate procedures on campus.
  - b. Reviewing and approving all proposed new or modified cash handling related applications, cash recording equipment, or methods of transporting cash.
  - c. Performing an annual review of compliance with these policies and procedures and informing the Associate Vice President/Controller of risks associated with each Campus cash-handling department

4. Disbursement Delegate(s)

The person or persons properly authorized to sign checks, drafts, or other orders for the payment of money or approve/release electronic transfers of funds against CSU checking accounts, provided that all such representatives are covered by fidelity bond.

5. Credit Card Acceptance Authority

The person properly authorized to act on requests concerning acceptance of commercial credit cards in payment of fees related to CSU activities.

6. Credit Card Coordinator / Internet Payment Gateway

The person who serves as the:

- a. 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, ensure the proper set up of these accounts from a vendor standpoint as well as an internal accounting standpoint.
- b. Record keeper of merchants operating on Campus, the equipment in place and services (merchant bank services and Internet payment gateway services) as used by each.
- c. Reviewer of credit card and payment gateway charges and qualification performance and who addresses problems with merchants as they arise to ensure the most cost-effective use of services.

V. CONDITIONS FOR EMPLOYMENT IN A CASH HANDLING ENVIRONMENT

Campus management must determine that all employees with direct cash handling duties, including temporary, casual, and student employees, have the background and character to accept responsibility and accountability for handling CSU cash and cash equivalents. *All employees who handle and process Cash and Cash Equivalents must be bonded by the CSU's bonding insurance.*

*The CSU carries fidelity bonds (with a high deductible) that protect it from losses associated with defalcations. These bonds provide coverage for all CSU 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.*

**Policy V.1:** Background checks are required for cashiers and other cash handlers; new employees' employment should be considered provisional until such a background check is completed. Any felonies, misdemeanors, or judgments that were due to fraud related to cash, stocks, bonds or any other financial transaction should be addressed immediately.

**Policy V.2:** Each department supervisor is responsible for arranging the appropriate background and employment verifications when hiring employees into critical positions. Before hiring a new cash-handling employee or finalizing a transfer into a critical position, the following must be completed:

- Employment history must be verified for all prospective employees.
- Background checks, supported by fingerprinting, to identify any prior criminal convictions must be completed.
- Other procedures may be conducted as deemed necessary by the Cash Handling Coordinator given the circumstances (e.g. credit checks).
- This documentation must be submitted to the Cash Handling Coordinator.

**Policy V.3:** Continuous bonding is an absolute condition for retaining cash handling responsibilities. If the cash handling employee's bonding cannot be maintained, the employee's cash handling responsibilities must be terminated. The requirements for bonding must be reviewed regularly for employees handling cash.

**Policy V.4:** If any employee having cash handling responsibilities is convicted of a felony or any crime related to cash, that conviction must be reported to Campus Police and Human Resources.

VI. MANAGING CSU BANK ACCOUNTS

**Policy VI.1:** Pursuant to the Standing Orders of the Board of Trustees of the California State University and a Delegation of Authority concerning the “Deposit, control, investment, expenditure, and lending of funds,” only the Office of the Chancellor has the authority to open, make changes to, or close official CSU bank accounts. Auxiliary organizations’ bank accounts are not subject to this requirement.

**Policy VI.2:** Only a Campus President or the President’s authorized designee (Campus CFO or the Associate Vice President and/or Controller) may recommend such requests.

**Policy VI.3:** Any bank account opened for CSU purposes but not established and authorized by the Office of the Chancellor must be immediately brought to the attention of the Campus Associate Vice President and/or Controller and CMO for resolution.

**Policy VI.4:** An annual search for unauthorized bank accounts shall be conducted by CMO.

VII. ESTABLISHING CREDIT AND DEBIT CARD MERCHANTS

CSU campus departments may make a request to the Cash Handling Coordinator to receive payment for goods and services by means of a Credit or Debit Card. CSU campus departments are encouraged to perform a “needs” analysis regarding the acceptance of Credit or Debit Cards at any point of sale.

- a. **Policy VII.1:** The Cash Handling Coordinator has the authority to accept or reject requests for Campus Merchant Card Services from campus departments.

**Policy VII.2:** Each Campus that accepts Debit and Credit Cards must develop its own rules and policies for the establishment of Credit and Debit Card Merchants (CSU campus departments acting as “vendors” providing services or selling goods to the campus community [Campus Merchants]).

When approving a department as a new Campus Merchant, the Cash Handling Coordinator will:

Determine whether the new Campus Merchant intends to accept Visa, MasterCard, American Express or Discover and whether it intends to accept both Credit and Debit Cards

Consider whether the new Campus Merchant is able to provide access to a telephone line that will permit automatic Credit and Debit Card processing by swiping the Credit or Debit card. Alternatively, determine the proper method of accepting Credit or Debit cards in the absence of a telephone line.

Determine if the Campus Merchant intends to accept Cardholder Present Transactions and make certain that the Campus Merchant has a secure means of storing the signature verification provided by the buyer/payer at the point of sale or payment.

Determine if the new Campus Merchant intends to accept Cardholder Not Present Transactions and make certain that the Campus Merchant has excellent record-keeping and can reassemble the transaction in the event of a dispute or a chargeback.

Determine whether the proposed Campus Merchant understands and can comply with the [Purchase Card Industry \(PCI\) Data Security Standards](#) compliance requirements.

Determine whether the proposed Campus Merchant understands the need to protect personal, sensitive information from disclosures and can meet the compliance requirements of the California Information Practice Act ([Senate Bill 1386](#)) and other similar regulatory requirements.

Determine whether the proposed Campus Merchant can deposit directly into a CSU bank account, or if the funds will be routed to a third party, and, if so, how long it will take for the funds to be deposited to an account in the name of and under the full control of CSU. Campuses may only choose third party handlers from an approved list of vendors, as provided by CMO.

**Policy VII.3 All Campus Merchant Card accepting locations must use an approved CSU Merchant Card processor.**

## VIII. PAYMENT TYPES

### Types of Payments Received (Cash, Cash Equivalents, and Checks)

#### A. Currency and Coin (“Cash”)

Currency and Coin are the most liquid of assets and must be immediately, and at all times, protected against loss. The physical security of Currency and Coin is crucial (See section X for policies concerning best practices for the security and safeguarding of Currency & Coin). Financial recording of Currency and Coin immediately upon receipt is an essential function that ensures employee accountability. Employee accountability requires that an individual knows **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 the beginning to the end of the cash-handling transaction cycle.

The following are unique requirements associated with Currency & Coin:

**Policy VIII.A.1: Large Dollar Transaction Reporting Requirements: Each Campus must comply with Federal and State Laws and Regulatory requirements associated with transactions involving currency and coin.**

The Internal Revenue Service (IRS) requires tax-exempt education organizations to report cash transactions exceeding \$10,000 (single transaction or accumulated by multiple transactions) received in the course of a trade or business, even if the income is not subject to the unrelated business income tax. The reporting requirement applies **only** to cash transactions. A Campus receiving a cash transaction for more than \$10,000 must complete and file IRS [Form 8300, Report of Cash Payments over \\$10,000 Received in Trade or Business](#), with the IRS on or before the 15<sup>th</sup> day after the date of the cash transaction, or two or more related business transactions that occur within a 15-day period. Consult IRS Publication 1544, [Reporting Cash Payments of over \\$10,000](#), for more information.

**Policy VIII.A.2: U.S. Dollar: A cash handling site will accept only United States coin and currency.**

#### B. Checks and Cash Equivalents (including Money Orders, Travelers Cheques and Certified Checks - see Appendix A for more information regarding these instruments).

The term “check” (including those instruments issued and commonly called warrants by the State of California) means any negotiable demand draft drawn on or payable through a United States office of a depository institution that is a qualified member of the United States’ Federal Reserve Bank.

**Policy VIII.B.1:** All checks must be payable to “California State University,” the “Trustees of California State University,” the campus name (i.e., San Diego State University) or reasonable variation on such names and must include:

- a. Dating no earlier than 180 days prior to the day of acceptance (unless a shorter time period is clearly marked on the face of the check) and no later than the day of acceptance
- b. Legible and consistent amount, both numeric and written
- c. Proper account holder signature.

**Policy VIII.B.2:** Checks and Cash Equivalents bearing the legend “Payable/Paid in Full” are not to be accepted.

**Policy VIII.B.3:** All documents requesting payments to the CSU must inform payers that their payments must be made payable to California State University, the Trustees of California State University, the campus name or reasonable variations on such names.

## IX. PAYMENT CHANNELS

In person/mail recording and receiving of cash and cash equivalents

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

**Policy IX.A.1:** Separation of duties must be maintained when cash is received. No single person should have complete control over the entire process of receiving, processing applying a payment, preparing the bank deposit and verifying the deposit.

**Policy IXA.1.1:** Tasks incompatible with cashiering shall not be performed by cashiers.

**Policy IXA.1.2:** The person collecting cash, issuing cash receipts, and preparing the departmental deposit shall be someone other than the person verifying the deposit.

**Policy IXA.1.3:** Mail remittances should not be verified as a payment to the CSU and then processed by the same employee.

**Policy IXA.2:** Individual Accountability must be maintained and documented for all Cash Handling Procedures:

**Policy IXA.2.1:** A unique identifier not accessible or shared with other people shall be assigned to each cashier and/or individual in a department. A cash register drawer, a cash drawer insert or another secure cash receptacle to which only the cashier has access will be provided. An individual endorsement stamp or its mechanical or electronic equivalent will be provided to allow for tracking of deposited and/or returned items back to the department and individual that/who accepted the items.

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

**Policy IXA.2.3** Documentation of cash differences must be maintained for each cashier.

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

B. Cash Receiving and Recording:

**Policy IXB.1:** In a timely manner, Checks and Cash Equivalents must be restrictively endorsed “for deposit only.”

**Policy IXB.2:** An official CSU 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 IXB.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. An uncleared collections cash received 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 IXB.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 IXB.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 IXB.5.1:** The receipts must be used sequentially and be inventory-controlled.

**Policy IXB.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 IXB.5.3:** All voided receipts must be retained (i.e., not given to the customer) and

have signed and/or electronic approval by a supervisor.

**Policy IXB.5.4:** Current day collections of Main Cashiering Stations must be deposited the same day, or at a minimum on the following business day.

**Policy IXB.5.5:** Collections at Satellite Stations and Departments must be deposited at the designated Main Cashiering Station or deposited with the bank directly at least weekly or whenever collections exceed \$500.

**Policy IXB.6:** Electronic Based Cashier Point of Sale Equipment must meet the CSU security and operational standards which are:

**Policy IXB.6.1:** All cash registers and point of sale equipment must produce a cash receipt with campus identifier for each customer.

**Policy IXB.6.2:** The equipment must have a feature for machine validation of cash-related documents.

**Policy IXB.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 IXB.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 IXB.6.5:** A unique identifier that is not accessible to other people must be assigned to each cashier/remittance processor. A cash register drawer,

**cash drawer insert, and an endorsement stamp or its mechanical equivalent must also be provided.**

**Policy IXB.7: A Remittance Processor (Lockbox) must meet the security and operational procedures of the CSU which are:**

**Policy IXB.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 IXB.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 IXB.7.3:** The remittance system must provide a unique identifier for each operator that is not accessible to others.

**Policy IXB.7.4:** The remittance system must endorse checks and verify individual cashier transactions.

**Policy IXB.7.5:** The remittance system must document all voids.

**Policy IXB.7.6:** The remittance system must have security in place so that previous day's transactions cannot be altered.

**Policy IXB.8: Checks drawn on foreign bank accounts that are not acceptable at face value by the depository bank must only be recorded as uncleared collections, and must be sent to an approved depository bank for collection. The Cash Handling Coordinator may approve the use of alternate, fully documented, procedures for the handling and recording of checks drawn on foreign banks.**

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

**Policy IXC.1: Cashiering sites that accept MasterCard, Visa, American Express or Discover Card and PIN based Debit Card transactions will use only Point of Sale technology supplied to the location by the Campus' Merchant Card processor.**

D. Point of Purchase ACH Requirements

**Policy IXD.1: 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.**

E. Sale of Admission or Event Tickets

**Policy IXE.1:** Sale of Admission or Event Tickets in person, procedures, standards and security must be equivalent to those stated in the Cash/Cash Equivalent Receiving and Recording Sections (Policies IXA-IXD).

**Policy IXE.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 IXE.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 IXF.1: Paper-based authority received in the mail to charge a customer's credit or debit card must use the following procedures:**

- 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 CVV or customer PIN numbers. It is advisable to store the data digitally, encrypt the data and grant access only to authorized persons with id and password protection.**

G. Accounts Receivable Conversion (ARC) ACH Requirements

**Policy IXG.1: 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.

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)

## H. Telephone

### 1. Credit/Debit Card Processing

Campuses may accept Credit and Debit card payments over the telephone. Such payments qualify for "cardholder not present" rules issued by the Credit Card Associations and mean that the ultimate risk of fraudulent payment instructions resides with the Merchant (in this case, the CSU). The process will work as follows:

**Policy IXH.1.1: The Credit or Debit card account number and CVV or PIN number must be supplied during the telephone conversation in combination with the expiration date.**

**Policy IXH.1.2: The correct billing address for the Credit and/or Debit card must be obtained.**

**The card information received in the 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 IXH.1.3:** 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 authorities. Pursuant to card association rules, do not retain/store the CVV or customer PIN numbers. It is advisable to store the data digitally, encrypt the data and grant access only to authorized persons with id and password protection. Please see [Purchase Card Industry \(PCI\) security standards](#) included in Policy VII.1.F or IX.J1. (See Appendix B for more information concerning Physical Security Guidelines).

2. TEL ACH Requirements

**Policy IXH.2.1:** NACHA enacted the TEL Standard Entry Code (SEC) for telephone-initiated ACH items with the following steps:

- a) 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 department 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.
- 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.

Through TEL, CSU departments can now originate ACH debits as payment from

any of their customers without requiring pre-enrollment.

I. Fax and Email

1. Credit/Debit Card Processing

**Policy IXI.1: Receiving payment instructions via a Fax transmission is prohibited as a violation of the intent of section 4(a) of the Uniform Commercial Code.**

J. Internet

1. Information Security

**Policy IXJ.1.1: Increasingly, the CSU will be accepting payments from customers over WEB-enabled connections facilitated by the Internet. The CSU subscribes to the [Purchase Card Industry \(PCI\) Data Security Standards](#). Accordingly, when any CSU department implements WEB-based payment methods (whether operating the system internally or through a third party), the department must comply with the following security standards:**

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

A more detailed description of the [standards](#) has been provided by [VISA.com](http://VISA.com).

2. Credit/Debit Card Gateway

**Policy IXI.2.1:** The CMO, in conjunction with Campuses, has developed the following policies and procedures concerning the use of [Credit/Debit Card Gateways](#). All CSU deployed Gateways must operate in conformity with prevailing PCI Data Security Standards and must be compatible with the CSU's Merchant Card processor.

3. WEB ACH

**Policy IXI.3.1:** CSU departments 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 CSU department that deploys WEB ACH must use a CSU approved service provider.

X. PHYSICAL SECURITY

**Policy X.1:** All cash and cash equivalents shall be physically protected from loss at all times.

**Policy X.2:** Excess cash (as determined by the Cash Handling Coordinator) must be removed from the cash register drawer during the business day and transferred to a secure cash handling area/vault.

**Policy X.3:** At the close of business, all cash must be secured as per Policy X.6 below.

**Policy X.4:** Deposits must be adequately protected from loss while in transit. When necessary, armored car service or police protection should be used (armored car service to be arranged through Cash Management Operations).

**Policy X.5:** 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 X.6:** Lockable receptacles or burglarproof/fire resistant safes to store cash and cash equivalents must be used 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 risk the loss of liability coverage from CSU insurance carriers.

**Policy X.7:** If more than \$2,500 in cash and cash equivalents is regularly on hand, a manual robbery alarm system or other appropriate measures 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 X.8:** If more than \$25,000 in cash and cash equivalents is stored, an automated alarm system is required to alert Campus police (or local police department for off site locations) if the storage area is entered after business hours.

**Policy X.9:** The combination of a safe must be given only to supervisory and authorized personnel who must then commit the combination to memory. A record of the combination, sealed and open only under double-custody to prevent undetected access, must be maintained away from the safe area. The Cash Handling Coordinator is responsible for keeping a record of the named individuals who know the combination to the safe.

**Policy X.10:** A safe must be opened in such a way that other persons do not view the combination.

**Policy X.11:** To the maximum extent practical, a safe must be locked between uses during business hours.

**Policy X.12:** A safe's combination must be changed whenever a person who knows the combination leaves the employ of a cash handling department. 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. The Cash Handling Coordinator is responsible for making these changes and retaining the documentation of changes.

**Policy X.13:** Each cashier must be provided with a separate lockable box or compartment in the safe to which only that cashier has access. Duplicate keys must safely stored away from the safe and be retrieved only under dual control.

**Policy X.14:** Funds or property not related to the operation of the CSU must not be stored in the safe/vault.

**Policy X.15:** 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 that meet the standards of that campus' security standards. 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 X.16:** Campuses will develop and deliver Cash handling training to all Cash handling employees:

- 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
- Cash handling staff will receive training on what to do in the event of a Campus emergency.

**Policy X.17:** Cashier operations should be included in Campus Business Continuity planning.

**Policy X.18:** Transporting deposits between cashiering sites or to the bank will be done in a secure manner in order to protect the financial assets and individuals involved in transport.

**Policy X.19:** Satellite Cashiering Stations, Cash Handling Departments and Accounting Offices may 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. In the case of cash deposits 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 just in case the deposit needs to be reconstructed.

XI. PREPARING DEPOSITS AND TRANSFERS TO BANKS

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

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

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

**Policy XIA.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 Satellite Cashiering Station.

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

**Policy XIA.5:** The Main Cashiering Station must record each deposit from a Cash Handling Department or Satellite Cashiering Station and issue a transfer receipt. 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 Satellite Cashiering Station no later than the next business day.

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

**Policy XIA.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. If the cash (coin and currency) portion of a single day's deposit from a campus exceeds \$200,000, the Cash Handling Coordinator is responsible for ensuring a notification is made to CMO the day of the deposit, either by telephone call or email. [cmo@calstate.edu](mailto:cmo@calstate.edu)

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

**Policy XIB.2:** Collections at Satellite Cashiering Stations and Departments shall be deposited at the designated Main Cashiering Station at least weekly or whenever collections exceed \$500.

**Policy XIB.3:** All bank deposits must be accompanied by appropriate documentation, such as a numbered deposit slip (see section IX for more information).

## XII. RECORDING TO THE GENERAL LEDGER

**Policy XII.1:** Deposits to banks must be reviewed, approved and recorded to the General Ledger in a timely manner.

**Policy XII.2:** All bank deposits must be accounted for in the General Ledger during the appropriate month.

**Policy XII.3:** Individuals with cash handling responsibilities may not prepare and post journal entries.

**Policy XII.4:** All journal automatic and manual entries must be reviewed and approved by designated employees in the Accounting Office. The preparer and reviewer/approver must be different persons.

**Policy XII.5:** 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 "uncleared collections" 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 "uncleared collections" must be in place.
- Separation of duties – the employee capturing and crediting the funds cannot reconcile the bank statements.

## XIII. 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 that 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 department 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 of returns are non-sufficient funds, account closed and stop payment. Checks returned to the Campus must be controlled during the process of attempting to collect on the returned amount. A non-cashiering department provides oversight over the returned Check process.

**Policy XIII.A.1: Cash Equivalents that are deemed to be uncollectible are to be returned by the depository bank to the designated non-cashiering department.**

**Policy XIII.A.2: Cash Handlers must not be involved in the returned Cash Equivalent process.**

**Policy XIII.A.3: The person who approves the requests for write-off of uncollectible Cash Equivalents must not maintain the inventory of returned Cash Equivalents.**

**Policy XIII.A.4: A returned Cash Equivalent must be redeemed by a new payment.**

**Policy XIII.A.5: The person maintaining the inventory of returned Cash Equivalents must not handle the cash received to redeem returned Cash Equivalents.**

**Policy XIII.A.6: No one person from the same office may perform more than one of the above functions.**

**Policy XIII.A.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 Debits

ACH debits may be returned unpaid by the banking system for a number of reasons; the primary causes of returned debits are non-sufficient funds, account closed, no authorization or authorization revoked. ACH debits returned to the Campus must be controlled during the process of attempting to collect on the returned amount. A non-cashiering department provides oversight over the returned ACH debit process.

**Policy XIII.B.1:** ACH debits that are deemed to be uncollectible are to be returned by the Originating Financial Depository Institution (depository bank) to the designated non-cashiering department.

**Policy XIII.B.2:** Cashiers must not be involved in the returned ACH debit process.

**Policy XIII.B.3:** The person who approves the requests for write-off of uncollectible ACH debits must not maintain the inventory of returned ACH debits.

**Policy XIII.B.4:** A returned ACH debit must be redeemed by a new payment.

**Policy XIII.B.5:** The person maintaining the inventory of returned ACH debits must not handle the cash received to redeem returned ACH debit.

**Policy XIII.B.6:** No one person from the same office may perform more than one of the above functions.

C. Credit/Debit Card Chargebacks

Credit and Debit Card returns, also known as Chargebacks, are the consequence of:

1. Unauthorized/fraudulent use of a credit or debit card
2. An unresolved dispute between the payer and the CSU
  - 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 CSU) overcharged for the good or service.

The Campus will be notified that cardholders' (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 CSU's Merchant Card processor to the Campus Merchant Card Account. The chargeback will identify the Merchant ID (which translates to a specific Campus business department) that accepted the payment and that Merchant ID will be debited for the returned item. The Campus Cash Handling Coordinator

is to notify the affected business department 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 department.

**Policy XIIC.2:** Cashiers must not be involved in the returned Credit/Debit Card chargeback.

**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.

#### XIV. THIRD PARTY RELATIONSHIPS (INCLUDES LOCKBOX)

The CSU 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 be needed to 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 CSU Cash, Cash Equivalents and ACH transactions requires extreme care in the selection and on-going management of such Third Parties. Accordingly, the following policies are necessary to safeguard CSU assets:

**Policy XIV.1:** The Chancellor Office’s Cash Management Operations must approve the use of any Third Party that is in possession of CSU assets to process CSU Cash, Cash Equivalents and/or ACH entries.

**Policy XIV.2:** Before entering into any relationship with a Third Party, a Campus must have Cash Management Operations perform an adequate review of the Third Party’s background, capabilities, financial condition and references.

**Policy XIV.3:** Third Parties that process Cash, Cash Equivalents and/or ACH transactions and actually have possession of CSU assets of less than \$100,000 per year must be reviewed for financial soundness and adequacy by Cash Management Operations no less than annually.

**Policy XIV.4:** Third Parties that process Cash, Cash Equivalents and/or ACH transactions and actually have possession of CSU assets in excess of \$100,000 per year must be reviewed for financial soundness and adequacy by Cash Management Operations no less than quarterly.

**Policy XIV.5:** Third Parties that assist the CSU or individual Campuses with management of Cash and Cash Equivalents must enter into a CSU approved Contract that requires, at a minimum, the same level of protection, regulatory compliance (including, but not limited to Purchase Card Industry [PCI] Data Security Standards and State of California Senate Bill 1386 privacy requirements), insurance, bonding, and accurate/timely handling of Cash, Cash Equivalents and/or ACH transactions and Data as is established for the CSU itself by this document. The CSU 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 CSU under Third Party Agreements must be approved by the Chancellor’s Office.

For more information see [Purchase Card Industry Data Security Standards](#)

Refer to California Information Practice Act ([Senate Bill 1386](#)) for privacy requirements

XV. PETTY CASH AND CHANGE FUNDS

**Policy XV.1:** Petty cash and change funds are provided as a service to operating departments that require such operating funds. Campus policies must be established to appropriately protect these funds from loss through the provision of safes, vaults or money chests for amounts exceeding \$100. The Campus Cash Handling Coordinator or the Campus Controller will approve the establishment of these funds

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

**Policy XV.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 XV.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, based on the amount in the fund, by someone other than the fund custodian, and verification of cash balances must be performed in the presence of the petty cash/change funds custodian and must be documented and maintained on file for the review of Internal Audit. The Cash Handling Coordinator or the Campus Controller will approve the procedures. .  
Frequency of cash counts is as follows:

<b>Size of Fund</b>	<b>Frequency of Count</b>
\$200 or less	Annually
\$201 to \$500	Quarterly
\$501 to \$2,500	Monthly
Over \$2,500	Monthly, if not prescribed more frequently by the Campus Cash Handling Coordinator

### **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 department by CSU’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 department’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 department ask to see the buyer’s/payer’s driver’s license.

The Cardholder Present model is beneficial to the CSU 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 department has collected the cardholder data (card number, name, expiration date, billing address) by telephone, or by WEB site. This transaction is completed when the buyer/payer provides the needed information to the CSU via a telephone, or WEB site and the CSU 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 give 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 CSU has a role in maintaining the integrity of U.S. currency. Campus personnel can help guard against the threat from counterfeiters by becoming more familiar with U.S. currency. Campus personnel should examine the money received closely. They should compare a suspect note with a genuine note of the same denomination and series, paying attention to the quality of printing and paper. Personnel should look for differences, not similarities.

If a counterfeit note is received:

- Do not return it to the passer.

- The cashier should write his/her 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 received 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 the campus if it is not a counterfeit note or will send 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 Cheques, Cashiers Checks, Certified Checks)**

Cash Equivalents, Money Orders; Travelers Cheques; 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 “California State University”, the Trustees of the CSU, or the campus name.

Specific information 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 CSU are to be issued payable to “California State University” Or the campus name.
- 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 payor should be asked to acquire a new Money Order for payment of any CSU 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 Cheques

**Travelers Cheques 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 Cheques can usually be replaced if lost or stolen. Travelers Cheques are generally considered “good as cash”. Travelers Cheques must be signed and made payable to the “California State University” or the campus name in front of the cashier or the recipient when presented at any CSU point of sale or collection. Travelers Cheques are available in different denominations and currencies. It is important to ensure that Travelers Cheques accepted by any CSU point of sale or collection are payable only in U.S. dollars.**

Note: Travelers Cheques are checks and are, therefore, subject to the stale dating rules of the Uniform Commercial Code. This means that a Travelers Cheque 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 Travelers Cheques older than 180 days. In most State jurisdictions, non-negotiated Travelers Cheques must be escheated to the State typically at the conclusion of year 2 or 3. Accordingly, Travelers Cheques older than 2 years should not be accepted and the payor should be asked to acquire a new Travelers Cheque for payment of any CSU obligation. Alterations cannot be made to a completed Travelers Cheque including the “Pay to the Order Of” and the dollar amounts.

### 3. Cashiers Check (also known as Official Check)

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, at the conclusion of 180 days. However, this rule is seldom actually enforced; special care should be used 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 payor should be asked to acquire a new Cashiers Check for payment of any CSU 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. Similar to 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 it “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 certification of the check is made 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 account holder sending funds (payer), or debits, originated by the account holder 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 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)<sup>1</sup>, accept and process “bill payment” instructions. Therefore, CSU 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 CSU

The CSU will be asked by clients or authorized by NACHA’s Operating Rules to debit client bank accounts as payment for goods or services. In each instance, the payor must give its authorization to the CSU 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 payor’s account through the ACH).

NACHA has established specific payment types (transaction codes) for each interaction with the client as briefly defined 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
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. Checks received from businesses or governments are not eligible for ARC treatment
PPD	Pre-arranged, Pre-authorized ACH debit to a client’s account.

## Automated Remittance Processing

The CSU departments may elect to operate either directly or through third party processors, automated remittance processing services (otherwise known as lockboxes). To be fully effective, these 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

<sup>1</sup> Key BSPs are firms like CheckFree, Metavante, e-Princeton, Authorize.net, Cybercash, etc.

(California State University, CSU, campus name, etc.), are dated correctly, are signed and are 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 safe kept in accordance with CSU data retention standards.

### Reason Codes for why Payment Types may be returned

Below is a chart highlighting the primary reasons why each of the payment types (in the left hand column) can be returned. For instance, every payment type, except ACH, can 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 CSU assets and technology resources that support the CSU enterprise is critical to the functioning of the CSU. CSU information assets are at risk from employee error, malicious or criminal action, system failure, natural disasters, etc. Such events could result in damage to or loss of information resources, corruption or loss of data integrity, interruption of the activities of the CSU, or compromise to confidentiality or privacy of members of the CSU community.

CSU 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 CSU constituencies and avoid any financial losses that may arise from the unauthorized use or disclosure of confidential information.

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

Refer to [Senate Bill 1386](#) for privacy requirements.

Specific Data Security guidelines for CSU 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 information unless it is absolutely necessary.
4. Restricted data elements, such as 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. 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 (for instance encryption), and that it is removed as soon as possible.
6. Do not e-mail restricted data, either in the body of an e-mail or as an attachment.

7. Encrypt restricted data in storage. Protect the encryption key from unauthorized disclosure.
8. Credit card account and transaction information must not be sent via unencrypted e-mail messages over the Internet. The CSU subscribes to the Payment Card Industry (PCI) Data Security Standards
9. Require Secure Sockets Layer (SSL) protocol for all credit card account and transaction information transmitted over the Internet.
10. 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 at least one external firewall.
11. 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.

#### **System and Data Access**

1. Access to the system should only be given 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 be deleted immediately when their job duties no longer require that access. A listing 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 the 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 sign in when not used for a reasonable amount of time. When you print restricted paper, pick it up immediately and shred when finished.
8. Change employee passwords regularly.