BRITE Training

About BRITE

The UCLA Health System Faculty Practice Group (FPG) directors and administrators initiated BRITE in May 2006. Training courses and user materials are offered in partnership with the UCLA Hospital System to support outpatient employees with job training and tools. The BRITE Training team aspires to assist UCLA Health System employees with reaching their performance goals.

Course Acknowledgements

A training course such as this one, involves many individuals who allocate time out of their busy work schedule to participate in the planning, design, and creation of training materials and activities. Their involvement contributes not only to the success of the training project, but to the success of all staff who attend. The BRITE team would like to thank everyone who contributed to the development of this new course.

Thank You for Caring!
UCLA Health System

Mission
The mission of the Faculty Practice Group (FPG) is to provide a structure, including policies and processes, to support the UCLA David Geffen School of Medicine faculty. The Faculty Practice Group’s primary mission is to provide a unified and integrated structure from which faculty can benefit. We support the academic mission of the David Geffen School of Medicine and offer excellent collaboration to our UCLA, University of California and community colleagues in support of our overall mission to create and transfer knowledge for the improvement of health around the world.

The mission of the UCLA Health System is delivering leading edge patient care, education, and research.

Vision
Healing humankind, one patient at a time, by improving health, alleviating suffering, and delivering acts of kindness.

Values
Compassion, Respect, Excellence, Discovery, Integrity, Teamwork.
**Course Introduction**

**Learning Outcomes**

- Demonstrate accountability; ensuring compliance to FPG cash procedures
- Understand why no single person is responsible for cash collecting, cash depositing, and cash accounting; Separation of Duties.
- Recognize if your office environment contributes to the safety of people and assets; Physical Security.
- Identify the cash handling policies for processing patient payments.
- Recognize the roles and responsibilities of cash handling.

**Learning Benefits**

- Learn the main principles of Internal Control.
- Know the different cash flow process of Sub Cashier vs. Main Cashier.
- Learn Cash Handling Roles.

**Agenda**

I. **Course Introduction**

II. **Cash Handling Process**

   - Cash Control
   - Cash Handling Roles
   - Change Funds
   - Principles and Practices

III. **Cash Handling Glossary**

IV. **Cash Handling Appendix**

   - Cash Handling Resources
   - Bus-49
   - UCLA Policy 360
   - UCLA Policy 361
   - C173-85
CASH CONTROL

The University of California maintains financial policies that comply with state and federal law, and incorporate recognized best practices for prudent oversight of the University’s financial assets. This manual explains 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 the Faculty Practice Group cash and cash equivalents. Its purpose is to ensure that these important assets are protected, accurately and timely processed, and properly reported.

Control Principles
The Faculty Practice Group has established certain basic internal control principles applying to collecting and accounting for cash and cash equivalents.

Accountability
The clinic manager is responsible for ensuring compliance to established Faculty Practice Group procedures for cash and cash equivalents that identify:

1. Which individuals in the outpatient practice receive cash and cash equivalents
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 in your practice who receives or has custody of cash and cash equivalents must be held responsible for cash and cash equivalents under his or her control.

Individual Accountability allows every transaction to be attributed to a specific individual, through unique process identifiers and separate cash receptacles accessible solely to that individual. *

Mechanisms that maintain accountability include the securing of funds, documentation of transfers, non-sharing of passwords, securing keys, linking all transactions to specific cash handling individual, providing each customer with a receipt for payment, uniquely locking cash drawer for each cashier and non-sharing of assigned safe combination.

*Back-up access should be accommodated solely via dual custody arrangements.
Separation of Duties
The clinic manager or designee is responsible for ensuring that no single individual is responsible for collection, depositing, and accounting for cash received in your practice. At least two individuals must carry out key duties of the cash handling process. The following functions should be separated to the extent possible: Record Keeping, Authorization, Asset Custody, and Reconciliation.

Record Keeping
Creating and maintaining department records is an integral component of cash handling. Record keeping is the task of all individuals assigned to the roles of cash collection, deposit preparation, and posting of deposits to subsidiary and general ledgers. Examples of record keeping duties are processing transactions (electronically or manually) and providing deposit records, and receipt copies to the FPG PBO for reconciliation purposes.

Authorization
Normally a supervisor, office manager, or department head, an authorizer is responsible for attesting to the validity of transactions. Examples of authorization duties are approving voids and other correcting entries, approving departmental deposits, approving movement of assets (e.g., cash, DME supplies, cosmetics, etc.) and approving exceptions, such as overages or shortages.

Asset Custody
The individual assigned to asset custody is responsible for ensuring that assets are secured in accordance with procedures and documentation. Examples of asset custody duties are having access to collected funds, change funds, safes, lock boxes, file cabinets, any additional locations where cash or assets may be stored, credit card receipts and manual downtime receipts.

Reconciliation
Duties generally performed at the supervisory level, FPG PBO and/or by Corporate Financial Services, reconciliation is the balancing of cash collected to cash posted in subsidiary and general ledgers. Some examples of reconciliation duties are comparing cash collections to cash balance report/receipts, comparing collections to deposits, and comparing funds collected to accounts receivable postings.
Physical Security and Data Transmission Security

The clinic manager or designee is responsible for ensuring that at all times that the safety of people and assets are the highest priority. Therefore, the clinic manager or designee must ensure:

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 information) are protected from loss, corruption, or compromise to confidentiality

<table>
<thead>
<tr>
<th>Physical Security Table</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Function</strong></td>
</tr>
<tr>
<td>Monitoring</td>
</tr>
<tr>
<td>Physical Layout</td>
</tr>
<tr>
<td>Personnel Pre-Screening</td>
</tr>
<tr>
<td>Inventory Control</td>
</tr>
</tbody>
</table>

⚠️ **Remember:** Physical security is effective when assets are properly stored, shortages / overages are monitored, keys are secured, cash counting is not visible by public, safe combinations are changed on a routine schedule, two employees are present for reconciliation, employee background checks are conducted and money transport occurs with either armored car, security or law enforcement personnel escort, depending on your location. Alarm systems are installed, if recommended by law enforcement or warranted based on BUS-49 standards

**Peak Periods**

Many FPG Ambulatory Practice offices and Hospital Services have periods when the amount of money they take in is substantially higher than the norm. Managers must evaluate the risk inherent during peak periods and determine which of the physical security requirements are cost effective for their office. A FPG best practice is to minimize the amount of cash stored overnight by making daily deposits and increase armored car pickup services to the bank/main cashier's station. Whenever an office has more than $2,500 in cash on a regular operating basis, an alarm system is required. Please reference BUS-49 for further detail on alarm
**Misappropriation of Assets**

Any unexplained shortages of cash should be considered a potential asset misappropriation. Such occurrences should be reported to FPG Management for referral to UC Police Department & Audit and Advisory Services Investigations Manager at 310-983-3735.

**General Policy**

It is best to open a safe away from public view and in a fashion that prevents others from observing the combination. A safe is to remain locked between deposits. Frequency of changing the safe combination should occur when a person that knows the combination leaves the employ of the office. In addition, the combination must be changed at least once a year. Documentation must be maintained showing the date and reason for the combination changes. BUS.49-IX.11

Safety for the employee and securing cash is improved when a second person is present when the office opens and again when closing the office for the day.

**Cash**

The University of California defines cash and cash equivalents as currency, checks, money orders, traveler’s checks, and cashier’s checks. The University of California also includes e-commerce in its definition of cash. E-commerce includes debit and credit ACH transactions and all other forms of electronic funds transfers (EFTs). All the cash and equivalents mentioned are treated the same and are referred to as cash. Be sure to include all forms of cash and cash equivalents when totaling total cash receipts for your location.

**Cash Handlers**

University of California policy BUS-49 defines the cash handling positions as: Cashier, Cash Handler / Preparer, Approver (typically a manager or designee), and Fund Custodian. There are dual terms that define the role of a Cash Handler. First, is the generic term—Cash Handler. Cash Handler identifies any person that handles or processes cash, regardless of frequency or dollar amount, and prepares deposits for verification by the Approver/Manager designee.

The University of California cash handling policy identifies persons that frequently handle cash, processes payments, and prepares deposits to a main cashiering station as a Preparer. In general, a Preparer operates the cash handling equipment, e.g. a credit card machine, Point of Sale (POS).

**Main Cashier Station**

As defined in the University of California cash handling policy, the term Cashier applies to any individual working in a sub or main cashiering station. The primary function of the Main Cashier Station is processing cash payments and preparing monies for direct bank deposits. There are three Main Cashier Stations at UCLA:

- Santa Monica /UCLA Orthopaedic Hospital Cashier’s Station
- Ronald Regan Hospital Cashier’s Station
- 200 Medical Plaza Cashier’s Station
Main Cashier Office
In the UCLA Health System Faculty Practice Group, a community-based office processing cash payments is a Main Cashier Office. There are approximately 40 Main Cashier Offices at UCLA operating cash handling equipment such as credit card merchant machines routinely making deposits to a Bank. Examples of offices at UCLA with this level of cash handling roles are:

- Faculty Practice Group (FPG) Community Practices
- Hospital Community Offices

Sub Cashier Office
In the UCLA Health System Faculty Practice Group, a campus-based office processing cash payments is a Sub Cashier Office of the Main Cashier Office. There are approximately 80 Sub Cashiering offices at UCLA operating cash handling equipment such as credit card merchant machines routinely making deposits to a Main Cashier Office. Examples of offices at UCLA with this level of cash handling roles are:

- Faculty Practice Group (FPG) Hospital Based Practices
- Faculty Practice Group Mapped Practices

Cash Flow Process
Cash from Faculty Practice Group operations have distinct deposit routes. Monies from a Main Cashier Office or Station get deposit directly into the bank while monies from a Sub Cashier Office are deposit to Main Cashier Stations.
Cash Handling Roles

If you are responsible for handling cash, you are accountable for the cash. You must comply with audit controls as stated by BUS-49 the University of California Cash and Cash Equivalents Received Policy, UCLA Policy 360 Internal Control Guidelines for Campus Departments, and UCLA Policy 361 Cash Handling Safety and Security. The primary cash handling roles for the Faculty Practice Group are Cashier, Cash Handler, Preparer, Approver (typically a manager or designee), and Fund Custodian.

Cashier
This person’s key duties are in a Main Cashier Station. The primary function of this individual is cash handling, payment processing and preparing deposits that go directly to the bank.

Cash Handler/Preparer
There are dual terms that define the role of a Cash Handler/Preparer. First, is the generic term–Cash Handler. This person’s main duties are in a Main Cashier Office or Sub Cashier Office. The primary function of this individual is cash handling, payment processing, and prepare deposits for verification by the Approver/Manager designee.

Note: Supervisors are accountable for ensuring that cash handling staff is knowledgeable of what to do in the event of a hospital emergency and that cashiering operations are included in disaster recovery planning.

Approver/Manager Designee
This person’s key duties are to approve cash reports/deposits, voided transactions, overages/shortages, and to reconcile deposits to Main Cashier’s Station validated receipts.

Fund Custodian
The person assigned to the role of Fund Custodian will be responsible for administering a change fund.
There are several processes involved with cash handling. Below is a brief description of action items that influence cash handling roles. As you review the list, reflect on how you would design a process in your office that recognizes the importance of each function in controlling the risks involved in cash handling.

- **Handling Cash**
  - Individual accepts cash payments, endorses checks and issues receipt; this individual has access to cash.

- **Preparing Deposit**
  - Individual counts cash and prepares departmental/Sub Cashier cash collections deposit form or bank deposit form; this individual has access to cash.

- **Reconciling Receipts to Deposit**
  - Individual comparing amount of cash collected based upon cash register tape totals, manual receipt book total, or receipt or admission number sequences to cash deposit amount.

- **Recording Deposit to General Ledger**
  - Individual approving the Departmental/Sub Cashier cash collections deposit form to ensure the individual preparing a deposit is different from the individual handling cash; this individual may not handle or have access to cash.

- **Making cash deposit**
  - Individual making cash deposit to either a main cashiering station or departmental cash handling station; this person has access to cash.

- **Comparing Deposits to General Ledger Entries**
  - Individual comparing amount of daily cash deposit appearing in monthly general ledger with amount recorded on miscellaneous cash receipt report; this person may not handle or have access to cash.
Following, are two charts demonstrating appropriate separation of duties in a two person and a three-person office.

**Separation of Duties**

<table>
<thead>
<tr>
<th>Three Person Cash Handling Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Role</strong></td>
</tr>
<tr>
<td>Individual #1</td>
</tr>
<tr>
<td>Individual #2</td>
</tr>
<tr>
<td>Individual #3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Two Person Cash Handling Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Role</strong></td>
</tr>
<tr>
<td>Individual #1</td>
</tr>
<tr>
<td>Individual #2</td>
</tr>
</tbody>
</table>
**CHANGE FUNDS**

Used by offices that collect professional fees or by offices that sell goods, change funds facilitate the ability to give change back to customers that pay in cash (currency or coin). Custodians of change funds are solely responsible for the funds entrusted to them. Four critical policy activities apply for staff delegated change fund responsibility: Accountability, Separation of Duties, Reconciliation, and Physical Security. The change fund custodian may be personally liable for losses due to custodian negligence.

Ensuring the funds balance and verifying the accuracy of totals, supporting documentation, and use of correct computations by the change fund custodian is often the responsibility of the office supervisor or designee. The process of verifying accuracy of totals and supporting documentation by the supervisor or designee is an example of the Separation of Duties.

Cash custodians are to ensure the amount of the change fund is accurate; an annual change fund reconciliation report is sent to AMCO for compliance.

Physical security of change fund stipulates securing the change fund when not in use. Secure funds up to $1,000 in a desk or file cabinet that does not use common campus locks (e.g., S-100 locks). Change funds in excess of $1,000 must abide by BUS-49 secure storage requirements.
**Principles and Practices**

Office leadership must ensure and authorize all Cash Handlers to handle cash. The procedure to authorize a person to handle cash is to verify employment history (new hires) or transfers and request an employee fingerprint and background check. University policy states that a background check is a pre-condition for delegating cash handling responsibilities. Individual accountability for cash shall remain consistent throughout all cashiering operations.

As a best practice, all departments should authorize in writing each individual responsible for handling cash in the office.

In principle, no one person should have complete control over a transaction. In practice, the separation of duties mandates at least two people are involved in any cash handling transaction.

**Some Practical Advice for Cash Handling**

Documenting the movement of monies is a critical component of the cash handling process. Each time a cash transaction occurs, proper documentation is the first step.

1. If payment is by check, ensure the check is payable to *UC Regents* or *The Regents of the University of California*. If by credit card, verify that the card is active. Record all payments with a receipt to the customer and place all cash and cash equivalents in a designated secure location. When receipt of payment is by mail, separation of duties requires at least three employees are part of processing remittances. One person opens mail, endorses checks, and logs payment. Another individual records the payment and the third person verifies receipt of the checks and deposits and code accounts correctly. Ideally, two people open mail together.

   All monies become the responsibility of the Regents of California. Upon receipt of a check, you must endorse it on the back before deposit with the main cashier’s station or with the bank. Endorse all checks payable to *UC Regents* or *The Regents of the University of California*

2. Control the amount of cash you have on hand. Count cash in a location outside of public view limiting others from knowing you are in possession of cash. At the end of the workday, secure all funds in a safe or locked receptacle. Leave the empty drawers open conveying the drawer contains no cash. To prevent too much cash from accumulating in your office, the University recommends to deposit excess cash at the Main Cashier’s Station located on the first floor of the Ronald Reagan Hospital, or 200 Medical Plaza, or to Santa Monica Hospital. Main Cashier Stations deposit directly to the bank. If office deposits meet or exceed $500, then you must deposit daily, but at least weekly regardless of amount.
3. Whenever money changes hands or accounts, both the individual handing off the money and the recipient must jointly count the funds and ensure to record the exact amount. Campus Corporate Financial Services will ensure that the cash received, recorded, and made for deposit equals the amount credited to our bank account. Regularly, compare the amounts reported on deposits slips to the amounts recorded in the General Ledger CashNet (BCR). Review Monthly deposit reports on the general ledger CASHNET at month’s end and report any discrepancies to Corporate Financial Services.

4. Whenever your cash and receipt amounts do not balance, the office manager or designee must investigate the differences to determine the source of the error. To investigate cash differences consider the following possible causes: Cash counted incorrectly. Recount the cash in dual custody. Run a second accounting tape to double check the accuracy of the first tape. What happens if you give too much change to the customer? If so, this is a shortage and the reason needs to be documented and reported. If you transpose numbers, double-check the numbers and slowdown in the future. Finally, if cash is missing, this is a loss and you must report it.

5. Staff working in a main cashiering office, will complete the bank deposit slip for Bank of America. Staff working in all other FPG Westwood, Santa Monica, and Hospital-based offices will complete a Departmental / Sub Cashier Cash Collections Deposit Worksheet. Correct usage of deposit slips/worksheets is very important. Offices that utilize adding machine tape(s) of all checks received and separate tape for credit cards transactions must attach corresponding checks and credit card receipts to the adding machine tapes. The preparer and reviewer must both sign or initial the deposit form.

**Things to Avoid**

The manual intends to raise your awareness of critical cash handling principles and practices to support the core values, ethics, and integrity of the UCLA’s Health System. A few items to avoid as you plan fiduciary responsibilities:

- Do not exchange checks for currency to make change for one another.

- Do not allow employees to cash checks for themselves or for co-workers.

- Do not allow or replace a deposit with a personal check.
CASH HANDLING GLOSSARY
**Cash Handling Terms**

**Authorize**
To agree to the commitment of funds for a specified use; authorization can only be given by a person who is responsible for the funds in question.

**Background Check**
A process conducted on volunteers and final candidates for critical staff/student position. The process includes an investigation of state and federal criminal history through the California Department of Justice (DOJ) Live Scan Fingerprinting process. Contact Staff Human Resources to schedule a background check.

**Call or Call Center**
A response to a merchant's authorization request indicating that the card issuer needs more information about the card or cardholder before a transaction can be approved; also called a referral response.

**Card Expiration Date**
See: Good Thru date

**Card Security Features**
The alphanumeric, pictorial, and other design elements that appear on the front and back of all valid credit and debit cards. Card-Present merchants must check these features when processing a transaction at the point of sale to ensure that a card is valid.

**Card Verification Value 2 (CVV2)**
A fraud prevention system used in card-not-present transactions to ensure that the card is valid. The CVV2 is the three or four digit value that is printed on the back of credit cards. Card-not-present merchants ask the customer for the CVV2 and submit it as part of their authorization request. For information security purposes, merchants are prohibited from storing CVV2 data.

**Cardholder**
The person to whom a credit card is issued.

**Card-Not-Present**
A merchant, market, or sales environment in which transactions are completed without a valid credit card or cardholder being present. Card-not-present is used to refer to mail order, telephone order, and Internet merchants and sales environments.

**Card-Present**
A merchant, market or sales environment in which transactions can be completed only if both a valid credit card and cardholder are present. Card-Present transactions include traditional retail - department, grocery, and electronics stores as well as boutiques, etc. - cash disbursements, and self-service situations, such as gas stations and grocery stores, where cardholders use unattended payment devices.
Cash
A term used in the UC cash handling policy that includes checks, currency, coin, e-commerce/ACH, money orders, securities, travelers checks, or other property easily converted to currency.

Cash Handler
There are two definitions for the term 'cash handler'. First is a generic definition that identifies any person who handles/processes cash as a cash handler without regard to frequency or dollar amount. In addition, the term, as used in the UC Cash handling policy, identifies specific persons who frequently handle cash, process payments and prepare deposits to a main cashiering station. In general, this person operates cash handling equipment, e.g. a credit card machine. In BUS-49, an office unit with this level of activity is called a sub-cashiering or Main Cashier office.

Cashier
As used in the UC Cash handling policy, this term refers to a person who works in a main cashiering station. The primary function of this individual is cash handling, payment processing and preparing deposits that go directly to the bank.

Change Fund
Cash fund used by a campus department to provide customers with change for transactions involving cash sales of departmental products or services.

Dual Custody
The involvement of at least two individuals in critical cash transactions or storage mechanisms to check each other and reduce the risk of a loss occurring.

Endorse a Check
To sign, stamp, or imprint the back of a check as evidence of the legal transfer of its ownership.

Fiduciary
1. Any person responsible for the custody or administration, or both, of property belonging to another, as, a trustee.
2. Of, relating to, or being a trustee or trusteeship.
3. Held in trust.
4. One such as an agent of a principal or a company director that stands in a special relation of trust, confidence, or responsibility in certain obligations to others.

Firewall
A security tool that blocks access from the Internet to files on a merchant's or third-party processor's server and is used to ensure the safety of sensitive cardholder data stored on a server.
**Fiscal Year**
The twelve-month accounting period ending on June 30 upon which the University's annual financial reports are based.

**Fund Code**
Five-digit accounting code, each representing a specific type of funding that may be used for a particular purpose.

**Fund Custodian**
A person who has been assigned responsibility for administering either a petty cash or change fund.

**General Ledger**
Central accounting record of an organization that contains the accounts that make up the entity's financial statements. Separate accounts exist for individual assets, liabilities, fund balances, revenue and expenses. In some cases, control accounts summarize detail appearing in a subsidiary ledger (for example, vendor balances tying into the accounts payable account). Official book of record for the UCLA campus consisting of balance sheet-related account balances, such as accounts receivable and accounts payable.

**GL**
An abbreviation for General Ledger (See above)

**Good Thru Date**
The date after which a bankcard is no longer valid, embossed on the front of all valid credit cards. The Good Thru date is one of the card security features that should be checked by merchants to ensure that a Card-Present transaction is valid. Also known as the Card expiration date.

**Guest, Official**
The person who renders a service to UCLA or attends a meeting, conference, or event at the invitation of the host.

**Individual Accountability**
For financial control purposes, individual accountability is the delegation of authority to qualified persons to initiate, approve, process and review business transactions and the holding of those persons responsible for the validity, correctness and appropriateness of their actions. Each individual's involvement who touched a transaction can be identified by computer ID, cashier ID on a cash register, handler ID on an endorsement stamp, signature or initials any of which uniquely identify the individual.

**Key-entered Transaction**
A transaction that is manually keyed into a point-of-sale device.
Location Code
One-digit accounting code representing the UC campus location; Santa Cruz campus is "7". Not typically used by UCLA departments.

Magnetic Stripe
The black stripe on the back of every credit card. The stripe contains magnetically encoded personal information of the cardholder as well as the credit card number. Comparing the credit card number on the magnetic stripe to the raised credit card number on the front of the card may identify a fraudulent card. A point-of-sale device electronically reads the information on a payment card's magnetic stripe when the card is swiped through the reader.

Mail Order/Telephone Order (MO/TO)
A merchant, market, or sales environment in which mail or telephone sales are the primary or a major source of income. Such transactions are frequently charged to customers' bankcard accounts. See also: Card-not-present.

Main Cashering Office
Term used by FPG to refer to Community Practice Offices that deposit directly to the bank.

Main Cashering Station
A campus unit/community practices who deposits directly to a bank. At UCLA there are three main cashiering stations:
1. The Main Cashier's Office Ronald Regan Hospital (RRH)
2. 200 Medical Plaza (200 MP)
3. SM UCLA Hospital Main Cashier Office (SMH)

Merchant Agreement
The contract between a merchant and a merchant bank under which the merchant participates in a credit card company's payment system, accepts credit cards for payment of goods and services, and agrees to abide by certain rules governing the acceptance and processing of credit card transactions. Merchant agreements may stipulate merchant liability with regard to chargebacks and may specify time frames within which merchants are to deposit transactions and respond to requests for information.

Payment Card Industry (PCI)
The association of credit card providers. PCI is also the association's abbreviation for the security requirements applicable to all merchants as the standard for protecting credit card information.

Petty Cash
A fund of money used to allow employees or students to make an immediate purchase of a low-value good or service from an outside vendor in situations where other campus purchasing alternatives cannot be used. Not to be confused with “CHANGE FUND.” Note: Some restrictions apply regarding the items that may be purchased.
Reconciliation
One of four critical policy activities. A variety of comparing or reconciling functions performed by unit personnel or Corporate Financial Systems staff to ensure that transactions are properly documented and approved, and assurance that appropriate individuals are involved.

Process used to confirm the accuracy of a balance appearing in a particular operating or general ledger account by comparing the balance to that which appears in another related, but independent data source, such as a bank statement balance or subaccount ledger summary total.

Record Keeping Duties
This includes all duties that result in the creation and maintenance of department records of revenue, expenditures and inventories. These records may be paper records or records maintained in an automated computer system.

Revenue
Income from the sale of products or services.

Review
Process of examining an account balance or a financial transaction for validity, appropriateness, reasonableness, accuracy, sufficient funding, timely recording, proper accounting coding, and/or authorization.

Sales Receipt
The paper or electronic record of a bankcard transaction that a merchant submits to a merchant bank for processing and payment. In most cases, paper drafts are now generated by a merchant’s POS terminal. When a merchant fills out a draft manually, it must include an imprint of the front of the card.

Secure Receptable
UC BUS-49 defines the requirements of what constitutes a secure receptable based upon the amount of cash routinely stored. Up to $1,000 can be stored in a locked desk, filing cabinet, etc. (Note: Avoid S-100 locks which are common on campus). Amounts of $1,001 up to $2,500 must be stored in a safe. Larger money amounts must be stored in a safe that meets the requirements stated in policy UC BUS-49 (pg. 9) and an appropriate alarm system installed to alert campus police. Only staff who have cash handling responsibilities should have access (via key or combination lock) to the secure receptable.
Self-Assessment
The PCI required annual review of procedures and processes to ensure compliance with current security standards. UCLA uses Trust Wave to administer the self-assessment questionnaire.

Separation of Duties
One of four critical policy activities, this is a division of responsibilities for the three functions that make up a process among various staff members to ensure that inappropriate transactions do not occur and any errors that are noticed are corrected. Duties that are separated include record keeping, authorization, asset custody and reconciliation. Separation of Duties is frequently referred to as Segregation of duties.

Sub-cashiering
As used in UC cash handling policy, an FPG Practice that frequently handles cash and routinely processes deposits to a main cashiering station.

Unsigned Card
A seemingly valid credit card that is not duly signed by the legitimate cardholder. Merchants cannot accept an unsigned card until the cardholder has signed it, and the signature has been checked against a valid, government-issued Photo ID, such as a driver's license or passport.

Voice Authorization
An authorization obtained by telephoning a voice authorization center.

Voice Authorization Center
An operator-staffed center that handles telephone authorization requests from merchants who do not have electronic POS terminals or whose electronic terminals are temporarily not working or for transactions where special assistance is required. Voice authorization centers also handle manual authorization requests and Code 10 calls.
# Cash Handling Resources

<table>
<thead>
<tr>
<th>Description of Service</th>
<th>Department</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assistance with cash process review</td>
<td>Cash Handling Liaison</td>
<td>310 983-3017 – Angie Price <a href="mailto:aprice@mednet.ucla.edu">aprice@mednet.ucla.edu</a></td>
</tr>
<tr>
<td>Background checks and scheduling fingerprinting</td>
<td>Staff Human Resources</td>
<td>Locate your Staff HR Service Team 310 794-0500</td>
</tr>
<tr>
<td>Cashiering questions/issues</td>
<td>Cash Handling Liaison</td>
<td>310 983-3017 – Angie Price <a href="mailto:aprice@mednet.ucla.edu">aprice@mednet.ucla.edu</a></td>
</tr>
<tr>
<td>Change Fund Request</td>
<td>General Accounting</td>
<td>310 794-8740 – Pat Romero <a href="mailto:promero@finance.ucla.edu">promero@finance.ucla.edu</a></td>
</tr>
<tr>
<td>Deposit Slips, Endorsement Stamp &amp; General Ledger assistance</td>
<td>General Accounting</td>
<td>310 794-2870 - Milae Kim <a href="mailto:mkim@finance.ucla.edu">mkim@finance.ucla.edu</a></td>
</tr>
<tr>
<td>Dunbar pickup &amp; Deposit bags</td>
<td>Administrative Cashier</td>
<td><a href="mailto:askamco@finance.ucla.edu">askamco@finance.ucla.edu</a></td>
</tr>
<tr>
<td>Evaluation or review of cashiering area security</td>
<td>Cash Handling Liaison</td>
<td>310 983-3017 Angie Price <a href="mailto:aprice@mednet.ucla.edu">aprice@mednet.ucla.edu</a></td>
</tr>
<tr>
<td>Police escort for transport of funds</td>
<td>Campus Police</td>
<td>310 825-1491 WW 310 319-3849 SMH</td>
</tr>
<tr>
<td>PRS setup</td>
<td>Financial Systems</td>
<td>310 794-2547 – Juana Osejo <a href="mailto:josejo@mednet.ucla.edu">josejo@mednet.ucla.edu</a></td>
</tr>
<tr>
<td>Report significant losses or discrepancies</td>
<td>Campus Police Audit &amp; Advisory</td>
<td>310 206-8126 WW 310 983-3737 – Sherrie Mancera <a href="mailto:smancera@iad.ucla.edu">smancera@iad.ucla.edu</a> 310 983-3017 – Angie Price <a href="mailto:aprice@mednet.ucla.edu">aprice@mednet.ucla.edu</a></td>
</tr>
</tbody>
</table>
Table of Contents

I. References ........................................................................................................................................ 3
II. Introduction ...................................................................................................................................... 4
A. Accountability .................................................................................................................................. 4
B. Separation of Duties ...................................................................................................................... 4
C. Physical Security and Data Transmission Security ......................................................................... 4
D. Reconciliation of Accounts ........................................................................................................... 5

III. Definitions ....................................................................................................................................... 5

IV. Roles and Responsibilities ............................................................................................................... 7
A. Office of the President .................................................................................................................. 8
B. Campus / Laboratory Locations .................................................................................................. 8
    Chancellor, Controller, Cash Handling Coordinator, Revolving Fund Withdrawal Designee(s),
    Credit Card/Internet Payment Gateway Coordinator

V. Managing University Bank Accounts ............................................................................................ 10

VI. Obtaining Approval to Accept Credit and Debit Card Payments .................................................. 10

VII. Handling Currency, Coin, and Checks ....................................................................................... 12
    Transaction Reporting Over $10,000 - Exemption ........................................................................ 12

VIII. Payment Channels – Required Controls .................................................................................... 14
    A. General Cashiering Policies for Receiving and Recording Cash and Cash Equivalents .......... 14
    B. Recording Cash and Cash Equivalents ..................................................................................... 15
    C. Point-of-Sale Equipment, Debit and Credit Card Processing ................................................... 17
    D. Point of Purchase and Back Office Conversion: ACH Requirements ....................................... 18
    E. Sale of Admission or Event Tickets .......................................................................................... 19
    F. Credit/Debit Card Batch Processing ......................................................................................... 20
    G. Accounts Receivable Conversion: ACH Requirements ............................................................. 20
    H. Credit/Debit Card Telephone Transactions .............................................................................. 21

Business and Finance Bulletins Home Page: http://www.ucop.edu/ucophome/policies/bfb/
I. Prohibition on Payment with Credit/Debit Card Via Fax Transmission ............................ 23
J. Payment with Credit/Debit Card Via the Internet .......................................................... 23

IX. Physical Security ............................................................................................................. 24

X. Preparing Deposits and Transfers to Banks ................................................................. 27
XI. Recording to the General Ledger ................................................................................ 28

XII. Returned Item Processing ......................................................................................... 28
  A. Cash Equivalents and Checks ..................................................................................... 28
  B. Automated Clearing House Debits .............................................................................. 29
  C. Credit/Debit Card Chargebacks ................................................................................ 30

XIII. Contracting with Third Parties to Process Payments ............................................. 31

XIV. Petty Cash and Charge Funds .................................................................................. 32

Appendix A  General Information on Accepting Payments ............................................. 33
Appendix B  Data Security ............................................................................................... 40
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-Revolver 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


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. 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.
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](http://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 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**

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

**Policy VIIIB.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

---

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:

- 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
- The payment amount is not readable, or the numerical amount does not match the written-out amount.
- The check is signed by someone other than the holder of the account.
- 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 VIII B.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 VIII B.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 VIII B.7:
If a Remittance Processor is used, it must meet the security and operational procedures of the University which are:

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

Policy VIII B.7.4:
The remittance system must endorse checks and verify individual cashier transactions.

Policy VIII B.7.5:
The remittance system must document all voided transactions.

Policy VIII B.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 VIID.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 VIII.E.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 VIII.E.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 VIII.E.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 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 VIII.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](https://www.pci-sq.com/) and in the attached Appendix B – Data Security):

<table>
<thead>
<tr>
<th>PCI Data Security Standard</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network</td>
<td>1. Install and maintain a firewall configuration to protect data&lt;br&gt;2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored data&lt;br&gt;4. Encrypt transmission of cardholder data and sensitive information across public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5. Use and regularly update anti-virus software&lt;br&gt;6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7. Restrict access to data by business need-to-know&lt;br&gt;8. Assign a unique ID to each person with computer access</td>
</tr>
</tbody>
</table>
2. Credit/Debit Card Gateway

Policy VIII.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 VIII.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 Handling 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 XIIIB.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 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 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 WITH 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 policies 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.
GENERAL INFORMATION

APPENDIX A

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 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 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:
  - Are equal to the amount of the check; and
  - 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:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEB</td>
<td>Internet originated ACH debit to a client’s account</td>
</tr>
<tr>
<td>TEL</td>
<td>Telephone originated ACH debit to a client’s account</td>
</tr>
<tr>
<td>POP</td>
<td>Point of Purchase originated ACH debit to a client’s account</td>
</tr>
<tr>
<td>BOC</td>
<td>Back Office Conversion</td>
</tr>
<tr>
<td>ARC</td>
<td>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</td>
</tr>
<tr>
<td>PPD</td>
<td>Prearranged, preauthorized ACH debit to a client’s account</td>
</tr>
</tbody>
</table>

\(^4\) Key BSP’s 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.

<table>
<thead>
<tr>
<th>Payment Type</th>
<th>Counterfeit/Altered Item</th>
<th>Non-Sufficient Funds</th>
<th>Stop Paid</th>
<th>Stale Dated</th>
<th>Account Closed</th>
<th>Fraudulent Endorsement</th>
<th>Not-Authorized</th>
<th>Product or Service Dispute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash Equivalents</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Checks</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>ACH</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit/Debit Cards</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Time Limits by which Payment Types Must Legally Be Returned

<table>
<thead>
<tr>
<th>Payment Type</th>
<th>Counterfeit</th>
<th>Non-Sufficient Funds</th>
<th>Stop Paid</th>
<th>Stale Dated</th>
<th>Account Closed</th>
<th>Fraudulent Endorsement</th>
<th>Not-Authorized</th>
<th>Product or Service Dispute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash</td>
<td>Days</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash Equivalents</td>
<td>24 hour reclamation</td>
<td>24 hour reclamation</td>
<td>24 hour reclamation</td>
<td>90 days</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Checks</td>
<td>24 hour reclamation</td>
<td>24 hour reclamation</td>
<td>24 hour reclamation</td>
<td>90 days</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACH</td>
<td>24 hour reclamation</td>
<td></td>
<td>24 hour reclamation</td>
<td>60 days</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit/Debit Cards</td>
<td>60 days</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.1 for 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.
UCLA Policy 360: Internal Control Guidelines for Campus Departments

Issuing Officer: Assistant Vice Chancellor, Corporate Financial Services
Responsible Dept: Financial Management Programs
Effective Date: July 9, 2001
Supersedes: UCLA Policy 560, dated 5/1/88

I. REFERENCES

II. PURPOSE AND SCOPE

III. STATEMENT

IV. ATTACHMENTS

I. REFERENCES

Source material for this policy has been drawn from the following resources.

1. UCLA Financial Policy, November 30, 1996;
2. UC Business and Finance Bulletin IA Series, Internal Audit:
   IA-001, Internal Control Standards Introduction,
   IA-101, Internal Control Standards Departmental Payrolls,
   IA-403, Internal Control Standards Issuance and Control of Operating Cash Funds;
3. UC Business and Finance Bulletin BUS Series, Business Affairs:
   BUS-43, Materiel Management,
   BUS-49, Cashiering Responsibilities and Guidelines,
   BUS-54, Operating Policy for University Supply Inventories;
4. UC Business and Finance Bulletin, RMP Series, Records Management;
5. UC Accounting Manual:
   A-000-7, Official Documentation Required in Support of Financial Transactions,
   C-173-61, Cash: Petty Cash Disbursements,
   C-173-78, Cash: Unclaimed and Uncashed Checks,
   C-173-85, Cash: Credit and Debit Card Program,
   C-557-21, Contracts & Grants: Cash Advance Programs,
   D-371-16, Disbursements: Approvals Required,
   D-371-36, Disbursements: Invoice Processing in Response to Purchase Authorizations
   (see also-UC Sales & Use Tax Manual), R-212-2, Receivables Management;
6. UCLA Cash Handling Security Policy, March, 1998;
7. UCLA Policy 740, Purchasing Goods and Services;
8. National Association for College and University Business Officers (NACUBO): Internal Control Questionnaire for Colleges and Universities;
II. PURPOSE AND SCOPE

An important part of the delegated accountability for the financial management of UCLA resources is the establishment and implementation of adequate internal controls. Internal control is a broadly defined process designed to provide reasonable assurance regarding the achievement of the following objectives:

- Ensuring the effectiveness and efficiency of operations;
- Safeguarding of assets against loss and unauthorized use or disposition;
- Ensuring the validity, accuracy and reliability of accounting records and financial reports; and
- Promoting adherence to prescribed management policies and procedures and regulatory requirements.

This policy describes the internal control components used to achieve the objectives noted above, and identifies those with responsibility for ensuring the efficacy of local guidelines designed to implement this policy and related policies of the University.

III. STATEMENT

A. Responsibility for Internal Control

1. Department administrators and managers are responsible for establishing and maintaining a system of internal controls, and for promoting a positive and supportive attitude toward them at all times by:
   - conducting or assigning to a designee required periodic review of departmental operating procedures to ensure that the principles and guidelines of internal control are being followed;
   - establishing controls where new types of transactions occur;
   - improving upon existing controls if control weaknesses are detected. See 2. below for responding to audit results and recommendations.

Because not all departments have sufficient resources to provide optimal control at all times, estimates and judgments must be exercised to assess the costs, benefits, and risks involved. The costs associated with internal control should not exceed the benefits derived. Given these considerations, administrators are strongly urged to adhere to the control guidelines contained in this policy as is practicable.

2. Audit and Advisory Services as well as external auditors, are responsible for reviewing the adequacy of departmental internal controls and for reporting their findings to the appropriate administrative levels within the University.
   - Department administrators and managers are required to take prompt and responsive action on all findings and recommendations made by both internal and external auditors.
   - The audit process is completed only after department administrators and managers receive the result of the audit, and action has been taken to (1) correct identified weaknesses, (2) produce improvements, or (3) demonstrate that management action is not warranted.
B. Internal Control Components

Internal control for the campus consists of five interrelated components. These are derived from the way a department administrator or manager runs an academic or administrative unit, and are integrated with the management process. The department manager has responsibility for ensuring and demonstrating that all five components of control are operating effectively.

1. Control Environment

The control environment set by a department administrator establishes the tone of the business unit, influencing the control conscientiousness of its employees. Control environment factors include an administrator's integrity; the ethical values and competence of his/her employees; the way an administrator assigns authority and responsibility, and organizes and develops the unit's employees. An administrator can help promote a good control environment by:

- holding regular team and one-on-one meetings;
- periodically evaluating staff training needs and providing for staff development;
- clearly communicating performance expectations to staff and providing periodic constructive feedback; and
- clearly articulating positions on ethical issues relating to business so that staff receive a clear, unambiguous message to act in an ethical manner.

2. Risk Assessment

Every administrator faces risks from external and internal sources that must be assessed. A precondition to risk assessment is the establishment of clear business objectives at all levels that are consistent and relate directly to those of the total organization. Risk assessment is the process of the identification and analysis of relevant risks to achievement of objectives, and forming a basis for determining how the risks should be managed. This should be a disciplined, documented and on-going process that is communicated to staff members as well as management.

3. Control Activities

The control activities are the implementing tools of internal control policy. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating procedures, security of assets and segregation of duties. The general guidelines for control activities are outlined below. Specific guidelines for applying these principles as they relate to departmental functions are presented in Attachment A.

   a. Separation of Duties

   Individual duties are separated so that one person's work routinely serves as a complementary check on another person's work. No one person has complete control over more than one "key" processing function or activity, such as authorizing, approving, certifying, disbursing, receiving or reconciling.

   b. Authorization and Approval

   Proposed transactions are authorized when they are proper and consistent with University policy and the organization's plans. Transactions are approved by the person delegated approval authority. Approval authority is usually conferred on the basis of some special knowledge or competency.
c. **Custodial and Security Arrangements**
   The responsibility for the physical security (custody) of assets is separated from the related record-keeping (accounting) for those assets. Unauthorized access to assets and accounting records is prevented.

d. **Review and Reconciliation**
   Departmental accounting records and documents 1) are examined by employees who possess sufficient understanding of the University financial system to verify that recorded transactions actually took place and were made in accordance with prescribed procedures; and 2) are compared with University financial system reports and financial statements to verify their reasonableness, accuracy and completeness.

4. **Information and Communication**
   Pertinent information must be identified, captured and communicated in a form and timeframe that enables a manager and staff to carry out their responsibilities efficiently. Information systems produce reports containing operational, financial and compliance-related information that make it possible to run and control a business or academic unit. Effective communication must also occur in a broader sense, flowing down, across and up the unit. All staff must understand their own role in the internal control system, as well as how individual activities relate to the work of others.

5. **Monitoring**
   Internal control systems need to be monitored -- a process that assesses the quality of the system's performance over time. Ongoing monitoring occurs in the course of normal operations and includes regular management and supervisory activities. In addition, separate operational evaluations are conducted based upon the assessment of risks and the effectiveness of ongoing monitoring procedures.

   Adequate supervision of personnel and other monitoring activities are required to ensure the reliability of accounting and/or operational controls by pointing out errors, omissions, exceptions and inconsistencies in the application of procedures.

**IV. ATTACHMENTS**

A. **Guidelines for Application of Internal Control Principles.**

   **Issuing Officer**

   /s/ Susan K. Abeles

   Assistant Vice Chancellor – Corporate
   Financial Services

   Questions concerning this policy or procedure should be referred to the Responsible Department listed at the top of this document.
ATTACHMENT A

Guidelines for Application of Internal Control Principles

The following are control activities, as described in section III.B.3. of Policy 360, for applying the internal control principles to the following departmental operations:

Accounting Records and Reports
The University financial system, which includes the University general ledger, subsidiary ledgers, and other management reports, provides most of the official accounting and financial records of the University. Many departments maintain supplemental records or produce management reports which often duplicate information contained on financial system reports.

To ensure the accuracy and integrity of departmental records and reports and to avoid making departmental decisions based on inaccurate or incomplete information, departmental personnel are expected to reconcile departmental records and source documents on a monthly basis with the University financial system ledger and other financial system reports.

After reconciling, any required adjustments and/or corrections must be made promptly. Such adjustments are documented by the employee assigned this responsibility.

Payroll
1. Separation of Duties
   A reasonable separation of duties should be established after considering the associated costs, benefits, and available resources. Under optimal conditions, no employee should have complete control over more than one of the following duties:
   a. Approving payroll transactions;
   b. Distributing payroll checks to employees;
   c. Reviewing payroll expense reports.

2. Authorization and Approval
   a. Personnel and payroll timesheets are approved only by employees formally designated with approval authority.
   b. Payroll transactions are entered by designated preparers. Preparer access is restricted via privileges specified in the Distributed Administrative Computing Security System (DACSS). After preparers enter the transactions, notices are then automatically emailed to reviewers via the Application System Authorization Process (ASAP). Preparers must understand all relevant regulatory requirements and UCLA policies and procedures as well as complete mandatory Personnel/Payroll training classes. Reviewers must review all transactions within two working days of receipt and resolve all questions that arise and ensure transactions are reversed until the questions are resolved.
   c. Approval authority is controlled through the Chief Administrative Officer (CAO) of each unit who is responsible for identifying individuals who will review and approve payroll changes via DACSS. The Departmental Security Administrator (DSA) is responsible for
the input into DACSS as directed by the CAO. Cancellation of privileges shall be promptly entered by the DSA when employees terminate or responsibilities change.

d. Departmental job and attendance records are approved each month by the staff employee’s supervisor and maintained on a formal and current basis. The original approved records are not returned to the employee for further handling after supervisory approval.

3. Custodial and Security Arrangements
   a. Payroll and related personnel records should be filed in a secure location with access limited to only authorized personnel.
   b. Payroll checks awaiting distribution to employees are kept in locked storage, accessible only to a check custodian (or alternate) formally assigned custodial responsibility.
   c. Check custodians require the presentation of proper identification before releasing checks to employees not known to them. When a payroll check is released to someone other than the payee, check custodians (1) require an authorization signed by the payee to release the check, (2) require proper identification of the person receiving the check, and (3) obtain a signed receipt which will be retained by the check custodian.
   d. Payroll checks that remain undeliverable after 15 days are returned to Corporate Financial Services, General Accounting, with an explanation of the delivery problem.

4. Review and Reconciliation
   a. Employees who possess overall knowledge of departmental accounts are assigned to review monthly payroll expense reports and the quarterly Personnel Activity Reports (PAR) to ensure the validity and accuracy of payroll charges. This reconciliation is documented by the employee assigned this responsibility.
   b. When payroll reporting deadlines require that time worked be estimated to the end of a reporting period, controls are established to ensure that the appropriate adjustments are made (after the fact) for differences between estimated and actual time worked.
   c. To ensure that final paychecks are accurately prepared for employees who have been placed in any status under which full standard pay is not to be received (such as terminations, separations, or leaves without pay), final time records are reviewed for accuracy prior to processing final transactions.

Purchasing, Receiving and Disbursements

1. Separation of Duties
   A reasonable separation of duties should be established after considering the associated costs, benefits, and available resources. Under optimal conditions, no employee should have complete control over more than one of the following duties:
   a. Placing orders;
   b. Approving purchase requisitions or purchase orders;
   c. Reviewing and processing invoices for payment;
   d. Reviewing and reconciling financial system reports or departmental appropriations and expenditures.
2. **Authorization and Approval**
   a. Transactions that ultimately will generate a disbursement or expense transfer are entered by designated preparers. Generally, for transmissions over $2,500 departments create and route them to Purchasing for the issuance of a purchase order (PO). For transactions under $2,500 departments have been delegated authority to place LVO’s (Low-Value Orders) directly with vendors (for exceptions to this general policy consult BUS-43). Preparer access is restricted via privileges specified in the Distributed Administrative Computing Security System (DACSS). Once preparers enter transactions, notices are automatically emailed to reviewers via the Application System Authorization Process (ASAP). Preparers must understand all relevant regulatory requirements and UCLA financial systems and policies. Reviewers must review all transactions within two working days of receipt and resolve all questions that arise and ensure transactions are reversed until the questions are resolved.
   b. Approval authority is controlled through the Chief Administrative Officer (CAO) of each unit who is responsible for identifying which individuals will review and approve transactions via DACSS. The Departmental Security Administrator (DSA) is responsible for the input into DACSS as directed by the CAO. Cancellation of privileges shall be promptly entered by the DSA when employees terminate or responsibilities change.
   c. The fulfillment of terms, the rates, and the charges related to services provided are compared to purchase requisitions, purchase orders, consulting agreements, and contracts.
   d. The issuance of a valid PAC order is authorization for Accounts Payable to process an invoice that is in accordance with the PO terms and University policy. As an added control, a department can specify that it wants to acknowledge receipt of goods or services prior to payment. If the receiving flag is set to “Y” when the order is placed, receipt acknowledgement must be entered into PAC electronically before payment can be released by Accounts Payable.
   e. The Accounts Payable processors review all invoices for payment to ensure that the accounts charged are proper and that payment has not previously been made.

3. **Review and Reconciliation**
   a. Employees who possess overall knowledge of departmental accounts are assigned to review monthly financial system reports to ensure the validity, accuracy and completeness of all current non-payroll expenditures. This review includes comparing current month expenditures to source documents. This reconciliation is documented by the employee assigned this responsibility.
   b. Original invoice and related backup documentation supporting the order purchases shall be retained by Accounts Payable.

**Inventories (Equipment and Supplies)**

Where applicable, these guidelines pertain to any inventory whose transfer, damage, disposal or loss would materially affect the value of the department’s assets and/or create serious departmental consequences.

1. **Separation of Duties**
   A reasonable separation of duties should be established after considering the associated costs, benefits, and available resources. Under optimal conditions, no employee should have complete
control over more than one of the following groups of duties:
a. Receiving, maintaining or issuing items;
b. Preparing and maintaining up-to-date records of the location, transfer, damage, disposal, or loss of inventory;
c. Performing annual physical inventory counts or inspections.

2. Authorization and Approval
   a. Requisitions approved by authorized departmental employees are required prior to issuing inventorial equipment or supplies.
   b. Any adjustment to inventory records (for returned, missing, damaged, obsolete or stolen items) is approved by departmental management. Large adjustments should be supported by written explanations.

3. Custodial and Security Arrangements
   a. Security arrangements used to safeguard inventory against loss through damage, theft, or misappropriation are proportional to its value and removability.
   b. With the exception of equipment purchased with the intent of off-campus use (such as laptop computers), off-campus use of University equipment shall be discouraged.
   c. Use of University equipment or supplies for purposes not related to work responsibilities at UCLA is not allowed.
   d. The fewest number of authorized employees possible shall have access to inventories. Locks, keys, and/or combinations securing movable inventorial equipment or supplies are changed whenever turnover occurs involving personnel who had access to these inventories. A record of keys and/or combinations is maintained by one departmental employee.

4. Review and Reconciliation
   a. Items are inspected for general condition, possible damage, and completeness, prior to their inclusion in the inventory. An employee with custodial responsibility for these items shall perform the inspection.
   b. Usage is reviewed regularly. Obsolete, inactive, or damaged items are removed from inventory in accordance with established procedures.
   c. A physical count of inventory should be taken annually. Management shall be advised of significant inventory discrepancies.

Cash Receipts

1. Separation of Duties
   A reasonable separation of duties should be established after considering the associated costs, benefits, and available resources. Under optimal conditions, no employee should have complete control over more than one of the following duties:
   a. Receiving and depositing cash (currency, checks or other negotiable instruments);
   b. Recording cash payments to departmental receivable records;
   c. Reconciling cash receipts to deposits and/or financial systems reports;
   d. Billing departmental customers for goods or services;
   e. System access to create journal entries to the general ledger.
2. **Authorization and Approval**
   a. University bank accounts may be established only with the approval of The Regents acting through the Office of the Treasurer. Campus requests for establishing University bank accounts are made through Corporate Financial Services.

   **B** Individual accountability for cash must be maintained throughout all cash handling operations from receipt through deposit. All transfers of accountability must be documented.

   c. Transfers of cash between two people are jointly verified in the presence of both.

   d. A departmental supervisor verifies and approves cash deposit and transmittal documents, voided transactions, and cash overages and shortages. Known or suspected misappropriations or mysterious disappearances of cash or securities must be reported promptly (See Business and Finance Bulletin G-29).

3. **Custodial and Security Arrangements**
   a. All cash must be physically safeguarded at all times in accordance with Business and Finance Bulletin, BUS-49, and the UCLA Cash Handling Security Policy which mandates the use of armored transport or armed escort during the transportation of cash to the Administrative Main Cashier or other major cashiering units, and the avoidance of transporting cash at night. Transportation of cash to central cash or branch banks will be by armored transport. Departments may not provide check cashing service.

   b. All documentation requesting payments to the University must inform the payers that their payments must be made payable to The Regents of the University of California, or to the UC Regents. Payee designations other than to The Regents must be approved through the Vice President-Financial Management in consultation with the Treasurer of The Regents. Accountability for each deposit transaction must be maintained.

   c. Departmental cash receipts must be deposited with a major cashiering station at least weekly or whenever collections exceed $500.00. In addition, collections must be deposited by fiscal year end (June 30). The amount of funds held overnight should be minimized.

   d. Checks and money orders are restrictively endorsed immediately upon receipt with a “UC Regents” stamp.

   e. Un-deposited cash receipts shall be kept in a locked receptacle (drawer, file, cabinet, safe, etc.).

     1. Security provided is proportional to the dollar amount of cash receipts being kept. (Refer to Business and Finance Bulletin, BUS-49, section V., I., or contact the Administrative Main Cashier for more detailed requirements.)

     2. Strict individual accountability for funds is maintained at all times.

     3. Keys and safe combinations must be given only to supervisory and authorized personnel who must commit the combination to memory. A recording of the combination must be sealed and maintained away from the safe area and is restricted to the fewest number of employees possible (of whom at least one shall be at a departmental supervisory or management level). For emergency backup access, a spare set of keys and/or a record of the combination shall be maintained in a locked receptacle in a manner that requires two people together to get physical access to the funds (dual-control).
4. Keys and safe combinations must be changed whenever a person having the combination leaves the employ of the department. In addition, the combination must be changed annually. Documentation must be maintained showing the date and reason for combination changes.

5. A record of keys or safe combinations issued shall be maintained by one departmental employee.

f. Cash receipts may not be maintained in departmental offices on a permanent basis, and may not be deposited in unauthorized or non-University bank accounts. Funds or property not related to the operation of the University must not be stored in departmental safes.

g. Disbursements shall not be made from cash receipts.

h. A departmental employee independent of cashiering operations opens departmental mail.

i. An employee independent of cashiering operations performs the follow-up and adjustment for returned checks.

j. Deposits must be adequately safeguarded while in transit; as required, armored transport service or police protection will be provided (see 3a. above).

k. A report of cash collections signed by the preparer must accompany each deposit to a major cashiering station from a cash handling department. An authenticated online report must be accessible to General Accounting, or a copy of the report signed by the preparer must be sent to General Accounting by the department on the day of the deposit. Supporting detail must be provided.

4. Review and Reconciliation

a. Cash receipts are recorded on the day received. Receipts issued should be preprinted and consecutively numbered.

1. Departmental accounting personnel are responsible for safeguarding and issuing receipt documents to cashiering personnel.

2. An original dated receipt is provided to the payer.

3. Copies of valid receipts and of voided receipts are kept for audit and reconciliation purposes.

b. Daily reports of cash receipts are subject to departmental supervisory review and approval.

1. Cash receipts are reconciled to deposits, and deposits are reconciled to financial system reports.

2. Cash shortages and overages are promptly reported to, and investigated by, the next higher administrative level.
**Petty Cash and Change Funds**

1. **Authorization and Approval**
   a. Petty cash and change funds shall be authorized and approved by Corporate Accounting.
   b. A fund may not be established from cash receipts that are not deposited to an authorized bank account.
   c. A fund is used only in accordance with the purposes agreed to at the time the fund is authorized and always conforms to established University policies and procedures.
   d. Check requests to reimburse a petty cash fund are approved by a responsible employee who does not have direct access to the petty cash fund. Fund reimbursement is made payable to the fund custodian.

2. **Custodial and Security Arrangements**
   a. Cash and cash reimbursement vouchers are stored in a locked receptacle (drawer, file, cabinet, safe, etc.). Security provided is proportional to the dollar amount of the fund.
   b. Custodial responsibility for a fund is assigned to only one employee. Custodial responsibility can be redelegated internally to cover absences of less than three weeks. The Assistant Vice Chancellor Corporate Financial Services must be notified in writing of redelegation when an absence exceeds three weeks.
   c. Petty cash is not to be deposited into an unauthorized or non-University bank account.

3. **Review and Reconciliation (Petty Cash Fund Only)**
   a. The fund custodian may not make any disbursements without first being presented with a receipt or approved reimbursement voucher documenting the expenditure.
      1. Original receipts are required in order to prevent duplicate reimbursements.
      2. Personal checks and IOU's may not be accepted as valid receipts.
      3. Any person receiving cash must sign an approved reimbursement voucher or receipt for cash received.
   b. The fund custodian shall balance the fund at least monthly and whenever the fund is replenished.
      1. Total cash plus reimbursement vouchers on hand should equal the authorized amount of the fund.
      2. Shortages or overages are reported and promptly investigated by departmental management.
   c. Funds are periodically verified through surprise counts.
4. **Review and Reconciliation (Change Fund Only)**
   a. The fund custodian shall balance the fund at least daily when in use.
      1. Total cash on hand should equal the change fund plus cash receipts.
      2. A change fund should have a constant balance. Shortages and overages should be reflected when depositing cash receipts and are reported and promptly investigated by departmental management.
   b. Funds are periodically verified through surprise counts.

4. **Billing and Accounts Receivable**

   The applicability of some parts of this section depends on the extent to which each department performs the billing and accounts receivable functions.

1. **Separation of Duties**

   A reasonable separation of duties should be established after considering the associated costs, benefits, and available resources. Under optimal conditions, no employee should have complete control over more than one of the following duties:
   a. Billing customers for goods or services provided;
   b. Collection;
   c. Establishing departmental credit policies; approving requests for credits, billing cancellations, billing, credits and write-off of debtor accounts;
   d. Receiving, recording and processing payments on receivables (cashiering functions);
   e. Reconciling receivable records to the financial system subsidiary ledger receivable reports.

2. **Authorization and Approval**

   Authorization and approval decisions regarding receivable functions are built into the Billing and Receivables (BAR) system and are in accordance with University Accounting Manual policies and standards.

   For non-BAR settings, receivable functions require approval by an authorized supervisory or management level employee when (a) establishing rate and/or billing schedules for charging customers, (b) issuing credit memos and/or billing cancellations, (c) granting credits to customers, or (d) determining which accounts are uncollectible and should be written off.

3. **Custodial and Security Arrangements**

   a. Departmental invoices are prepared and issued only by authorized personnel.
   b. For BAR applications, invoices are system generated and are assigned numbers in sequential order. Charge and payment transactions are recorded and maintained in the system. For non-BAR applications, invoices are issued in numerical sequence. Copies of voided invoices are kept for audit and reconciliation purposes.
   c. For BAR applications, charge reversals are restricted by system security. For non-BAR applications, blank invoices, credit memos, and cancellation forms are controlled exclusively by personnel assigned invoicing responsibilities.
4. **Review and Reconciliation**

   a. Monthly financial system subsidiary ledger receivable reports are reviewed by staff with overall knowledge of receivable management. This reconciliation is documented by staff assigned this responsibility.

   b. Delinquent account balances are examined and follow-up with customers is initiated to determine reasons for non-payment. If a reasonable or satisfactory explanation is not received from a debtor regarding the delinquent account, the debtor is precluded from receiving additional credit.

   c. Departmental billing records are periodically compared and reconciled to account balances appearing on financial system subsidiary ledger receivable reports.
I. REFERENCES

1. UC Business & Finance Bulletin BUS-49, Policy for Cash and Cash Equivalents Received;
2. UCLA Policy 360, Internal Control Guidelines for Campus Departments.

PURPOSE

UC Business & Finance Bulletin (BFB) BUS-49 establishes the minimum requirements related to the handling and processing of cash and cash equivalents to ensure that these assets are protected, accurately processed and properly reported. Each campus is expected to adhere to these minimum requirements and establish local implementing procedures accordingly. In addition, UCLA is committed to ensuring that those engaged in the handling and transporting of cash are protected and that associated risks are minimized. This policy covers basic practices for the campus for the safe and secure handling and transporting of cash and cash-like assets by authorized individuals and units.
III. DEFINITIONS

**Armed Escort**: UC Police officer or professional armed security guard employed by the UC Police Department who accompanies any person engaged in Cash handling activity.

**Campus Cashier Coordinator**: The Director of Student Financial Services, who is responsible for coordinating all UCLA cashiering operations, including those of ASUCLA.

**Cash**: For purposes of this policy, includes checks, currency, coin, credit/debit card recordings, bank notes, bullion, traveler’s checks, registered checks and money orders.

**Cash Handling Site**: Any on or off campus department or location from which Cash is deposited to a cashiering station.

**Main Cashiering Station**: A designated location to which authorized operating Cash funds are issued and from which Cash collections are deposited directly to any bank.

**Sub-cashiering Station**: A designated location from which Cash collections are deposited to a Main Cashiering Station.

IV. STATEMENT

1. There shall be no nighttime transports of Cash except when circumstances make such transport unavoidable.

2. When a nighttime (dusk to dawn, Monday through Friday) transport is unavoidable, the Cash will be picked up by an armored courier service contracted to provide Cash transport services to the University, or delivered to an appropriate cashiering station by an authorized Cash handler who is accompanied by an Armed Escort.

3. Nighttime or weekend (Friday dusk to Monday dawn) deposits of Cash remaining at a Cash Handling Site shall be safeguarded in compliance with BUS-49 to the greatest extent practicable.

4. Daytime (dawn to dusk, Monday through Friday) Cash collections or deposits shall be safeguarded in compliance with BUS-49 to the greatest extent practicable.

5. Transport of Cash from Sub-cashiering Stations and other Cash Handling Sites to a Main Cashiering Station shall be by Armed Escort or authorized armored courier service.

6. Transport of Cash from Main Cashiering Stations to a Los Angeles central cash vault or branch bank shall be by authorized armored courier.

7. All cashiering stations are subject to periodic site surveys in order to evaluate the adequacy and effectiveness of the physical security of each station. Other Cash Handling Sites shall be evaluated periodically with the goal of maximizing the safety of the Cash handlers therein.

Based on results of the site surveys, the Campus Cashier Coordinator shall specify the provisions for the appropriate upgrading of Cash Handling Sites including, but not limited to, anchored safes, bullet-proof glass, alarms and/or emergency communication equipment such as two-way radios or cellular phones.
Department staff with responsibility for Cash handling operations shall ensure that all required safety provisions are implemented for their respective Cash Handling Sites.

8. Public notices that declare the presence of security provisions and lack of cash accessibility shall be displayed at cashiering stations and other Cash Handling Sites where applicable (e.g., signs proclaiming the presence of alarms, that the safe cannot be opened by employees, that cash is not collected at the gates of certain public events, etc.).

Any deviation from the related provisions of BUS-49 and UCLA Policy 360 or this Policy must be approved in advance by the Campus Cashier Coordinator and shall be documented. Departments, in consultation with the Campus Cashiering Coordinator, may adopt more stringent safety measures as appropriate for their area.

Questions concerning implementation of these procedures should be directed to the Student Financial Services Director at (310) 206-6034.

Issuing Officer

/s/ Susan K. Abeles Associate Vice Chancellor, Corporate Financial Services/Controller

Questions concerning this policy or procedure should be referred to the Responsible Department listed at the top of this document.
Policy C173-85

CASH: CREDIT AND DEBIT CARD PROGRAM

ACCOUNTING MANUAL

TL 64 3/31/95
CREDIT AND DEBIT CARD PROGRAM

Contents

I. Introduction
   A. University Policy
   B. Definitions

II. Card Services Controls
   A. Agreement with CES
   B. Authorized Officials
   C. Campus Card Program Coordinator
   D. Eligibility to Accept Cards
   E. Establishment of Cards and Services

III. Processing
   A. Deposit Options
   B. Other Services
   C. Equipment
   D. Service Fees and Billing
   E. Merchant Operating Procedures

IV. Procedures
   A. Depository and Drawdown
   B. Chargebacks
   C. Reconciling the Bank Account

V. Responsibilities
   A. Authorized Official
   B. Campus Card Program Coordinator
   C. Accounting Office
   D. Cashiering Stations/Merchant

VI. References

Exhibit 1: Sample Notification Letter
Appendix A: List of Authorized Officials
I. INTRODUCTION

This chapter presents University policy and outlines procedures pertaining to the authorization granted to certain approved University activities to accept credit and debit cards as payment for services performed, or for merchandise sold by such activities. The procedures for implementing this policy and the provisions of the agreement executed by the Office of the Treasurer between The Regents and Card Establishment Services, Inc. (CES), the University's card processor, are detailed below.

II. UNIVERSITY POLICY

The Regents established the policy that the appropriate use of commercial credit cards should be administered at the system wide level and authorized the President to approve University activities for card usage. Subsequently, with Regents' approval, President Saxon delegated the authority to Acting Vice President Cheit. In July, 1993, President Peltason expanded this authority to include the Chancellors and Laboratory Directors. This authority may be re-delegated to a specific designee, but may not be further re-delegated. The Regents' Bylaws grant the Treasurer of The Regents the authority to execute agreements on behalf of the University, in connection with banking type services provided by entities other than banks.

III. DEFINITIONS

The following terms used in this chapter are defined below:

1) **Card** refers to unexpired VISA, MasterCard, Diner's Club, American Express, Discover, JCB, etc. credit cards. It also includes debit cards from bank associations with networks, such as Maestro and Interlink.

2) **Merchant** is defined as a campus department or an activity of the University that has received the appropriate authorization to accept Cards in payment for services performed or for merchandise sold by the University.

3) The **cardholder** is the person whose name is imprinted on the Card, or whose name appears thereon as an authorized user.

4) A **chargeback** is a transaction that has been returned, due to a deposit error or cardholder dispute, resulting in a debit to the campus bank account. The term also refers to items returned due to lack of adherence to the conditions of the agreement with CES, or to Card Association and Debit Network regulations.
IV. CARD SERVICES CONTROLS

A AGREEMENT WITH CES
The CES Agreement executed with CES by the Office of the Treasurer, which regulates the use of Card services, is applicable to all nine campuses, the three Laboratories, and the Office of the President. Significant provisions of the agreement are outlined in Section V. of this chapter. University affiliated organizations that maintain separate bank accounts also must comply with the conditions of this agreement.

B AUTHORIZED OFFICIALS
CES accepts requests to establish Card usage and add new services from Authorized Officials for each location. An Authorized Official is an individual delegated the authority to approve requests to establish Card usage. This includes the authority to approve other services offered by CES, as detailed in section IV.E.2. below. Appendix A contains a list of Authorized Officials. As specified in Section II., any re-delegation of this authority must be made in writing, and copies sent to the Office of the Senior Vice President-Business and Finance and the Special Assistant-Coordination and Review. In addition, a copy must be sent to the Office of the Treasurer, Operations, in accordance with the provisions outlined in the Regents' Bylaws, Section

C. CAMPUS CARD PROGRAM COORDINATOR
CES requires that a single contact person be designated to manage the Card program on each campus. Therefore, each campus must designate a Card program coordinator in the accounting or cashiering office to provide information and assistance to departments considering the establishment of Card services, and to act as a liaison between campus departments and CES. The Card program coordinator will assist departments with requests to establish new cards and related services

D. ELIGIBILITY TO ACCEPT CARDS
Only those activities that can justify the need to accept Cards are eligible to establish Card services. Normally, such a need is justified if the acceptance of cards will increase net revenues. Therefore, eligible activities primarily consist of self-sustaining activities with a significant sales volume; thus, the fact that a cashiering activity collects income is not an adequate justification for Card use
E. ESTABLISHMENT OF CARDS AND SERVICES

1. Request For Approval to Accept Cards
   Each request for approval to accept Cards will be considered on its own merits. Such requests must be made in writing to the appropriate Authorized Official (see list in Appendix A).

2. Card Arrangements
   Upon approval, the Authorized Official will notify CES of the authorization (with copies of the letter provided to the campus Card program coordinator and the Office of the Treasurer, Operations). (See sample notification letter in Exhibit 1.) CES will contact the campus Card program coordinator to make arrangements for equipment, a merchant number, etc. and will formally notify the Authorized Official regarding the arrangements that have been made for the establishment of cards and services. Imprinters must bear the campus name and the merchant identification, in addition to the unique merchant number, as follows:

   Merchant Number
   UCSD-Ticket Office
   La Jolla, CA. 92093

V. PROCESSING

A. DEPOSIT OPTIONS
   In accordance with the CES agreement, there are four methods available to the Merchant for processing Cards:

1. Electronic Data Capture
   Terminal Card Reader This method of processing Card transactions is the most inexpensive credit card processing method available. As in option 2 below, Merchants reconcile all transactions processed through CardNet to the actual sales draft for each batch processed and submitted to CES. Paper copies must be maintained for a minimum of seven (7) years. This method should be considered by a merchant who uses a computer with communication capabilities. The primary difference between this option and option 2 is that the Card is normally presented to the merchant processing the transaction.

2. Electronic Data Capture
   PC Batch Under this method, CardNet terminals are used to obtain authorization to accept Cards and to make deposits, thus eliminating the need for manual deposits. The CardNet terminals utilize PC Retail, a software product viewed through a Windows environment. Under this option, a given transaction can be captured immediately for credit by CES. All transactions processed through PC Retail are reconciled by the Merchant to the actual sales draft, for each batch processed and submitted to CES. Paper copies are maintained at the campus location and must be available for a minimum of seven (7) years, in accordance with Federal and State laws. Although there are other uses for this option, phone and mail orders, as well as in-house processing, are the most appropriate. Typically, Cards are not presented to the Merchant when this method is used.
V. PROCESSING (cont.)

3. Paper Processing/Data Capture (In-house Processing Center)

This method, which is a two-step process, is preferable to option 4 below. It requires Merchants to forward their sales drafts to a central location for data capture (see option 2 above).

If a campus has several Merchants processing sales drafts manually, an In-house Processing Center may be set up to eliminate the need to mail sales drafts to CES.


This is a manual method of depositing and acquiring approval for Cards, and should conform to the provisions of Accounting Manual Chapter C-173-14, Cash: Campus Cash Collection Deposits, and Business and Finance Bulletin BUS 49, Cashiering Responsibilities and Guidelines. This is the only method that requires a Merchant to mail all sales drafts to CES daily for processing. According to the CES Agreement, CES will not be liable for any sales drafts lost en route to them, or for any chargebacks arising from transactions that are manually processed. Thus, since this procedure poses the risk of financial loss to the University, it is not recommended.

If this option is chosen, the request for approval (see section IV.E.1.) must include the Merchant's intention to use this option. The total costs involved, the number of Card transactions anticipated, and the Merchant's needs should all be considered in determining whether this option is suitable.

The CES Agreement requires that all transactions submitted manually must contain a merchant identification number, an authorization code, and an imprint of the Card, which should include the card number, the Card expiration date, and the cardholder's signature.

B. OTHER SERVICES

The CES Agreement includes the following additional services for assistance in the implementation of a Card Program.

1. CES Image

CES Image is an electronic archival record management service that creates a paperless processing environment. A cardholder signs on a glass display using an electronic personal identification number and receives a paper receipt. Campus accounting offices and merchants can obtain copies of the transaction from CES upon request.

2. CES Link

CES Link, a software product that provides information that can be viewed through a Windows environment, is essential to accounting offices. It provides access to information regarding authorizations, deposits, chargebacks, payments, and settlements. It provides Merchants and accounting offices with access to the daily and monthly activity of Cards processed through CES. CES Link provides the information needed to reconcile campus bank accounts.
Historical information is available for a six month period. For an additional fee, CES Link also provides a chargeback pre-notification service. Subscribers have access to a list of outstanding, expired, and resolved chargebacks, and are allowed fifteen calendar days to respond to a chargeback before the bank account is debited. (CES Link requires DOS 3.1 or a later version of DOS, and Windows 3 or a later version.).

3. Debit Card

Debit cards allow merchants to accept ATM cards for payment of goods and services. CES supports major debit networks including, but not limited to, Most, NYCE, MAC, Honor, Pulse, Cash Station, Interlink, Explore, BankMate, and Maestro. Online debit services provide for authorization/capture, reversal, return, clear, cash back, and batch recovery.

4. SCAN Check Verification System

SCAN is a check verification system that can be used to reduce the number of bad checks. SCAN does not guarantee or authorize a transaction; rather, it functions like a national clearinghouse to collect and distribute information concerning bad checking accounts. CES maintains twenty-four hour availability to SCAN, except for a one-hour system maintenance period every Sunday morning between midnight and 3 a.m.

C. EQUIPMENT

Most of the equipment needed to process Cards can be provided by CES. If the equipment is rented, CES will maintain, repair, and modify the equipment, as needed. Any equipment that is rented or sold by CES may be programmed only by authorized CES personnel. (See CES Operating Procedures Guide).

D. SERVICE FEES AND BILLING

Settlement for MasterCard and Visa fees, rental of equipment, and fees for network access are billed monthly. The frequency of billing for other fees can be determined by each campus.

E. MERCHANT OPERATING PROCEDURES

Operating procedures under the CES Agreement are described in the CES Operating Procedures Guide. The focus of the Guide is to help train cashiering employees to accept Cards with a minimum risk of chargebacks. CES will provide accounting offices and Merchants with copies of the Guide.

VI. PROCEDURES

A. DEPOSITORY AND DRAWDOWN

Each campus must have a separate bank account for Card transactions, at a bank specified by the Treasurer. The campus accounting office receives a monthly statement from the bank which includes a daily total deposit amount, comprised of various merchant deposits and chargebacks. Transfers to the Treasurer's Concentration account from the campus account also appear on the statement.
1. **Deposit**
   The merchant prepares a University Bank Deposit Receipt form for each deposit (see example in Accounting Manual chapter C-173-14). If the deposit form required by CES or other processor is pre-numbered, campuses may use that form instead of the University Bank Deposit Receipt form. However, if such a departure from procedure is elected, strict deposit receipt control must be maintained.

   The supporting detail for deposits and chargebacks is provided by CES through CES Link (see section VII.B.2., below). If a merchant or campus accounting office does not choose CES Link services for verification of receipt of deposits, paper reports of Card activity will be provided by CES.

   Card deposits prepared and deposited by Merchants are recorded in the campus General Ledger as follows:

   
   DR: X-1100XX Campus Cash Account  
   CR: X-XXXXXX Merchant Account

   The CES Operating Procedures Guide provides specific requirements regarding deposit forms to be used for deposits made through the mail and data capture, with instructions for ordering these forms

2. **Drawdown**

   CES, through its bank, will transfer funds to the appropriate campus bank accounts. The campus depository bank transfers these funds into the Treasurer’s Concentration account; the funds will be recorded in the Treasurer’s Report on the day after the transfer is made. Subsequently, the campus is notified by the Office of the President (OP). The following entries to record the transfer are required:

   **OP Accounting Office Entry**

   DR: J-110000 Treas General Cash Acct  
   CR: J-1195X0 Financial Control Account

   **Campus Entry**

   DR: X-119500 Financial Control Account  
   CR: X-1100XX Campus Cash Account

   CASH: CREDIT AND DEBIT CARD PROGRAM

B. **CHARGEBACKS**

   Campus accounting offices will be notified of chargebacks through CES Link or paper reports. All debit and credit adjustments related to these chargebacks must specify the reason for the return. The campus accounting office is responsible for notifying the appropriate Merchant of the returned item so corrective action can be taken and the appropriate accounting entries made.
C. RECONCILING THE BANK ACCOUNT

The campus bank account should be reconciled on a monthly basis by a designated person in the campus accounting office. The campus General Ledger Cash Account is the official University record, and its balance should be used as the control to reconcile the bank balance. Discrepancies between the CES bank account statement and the campus bank account statement should be directed to CES.

VII. RESPONSIBILITIES

A. AUTHORIZED OFFICIAL

The Authorized Official is responsible for approving an activity's request to establish cards and services.

B. CAMPUS CARD PROGRAM COORDINATOR

The Card program coordinator is responsible for maintaining records regarding equipment and services provided by CES, and for providing assistance and advice to campus users.

C. ACCOUNTING OFFICE

The accounting office is responsible for the following:

1. maintaining control of all Card deposits, for the purpose of identifying specific Merchant locations. If a receipt is missing, the accounting officer must take immediate action to account for it;
2. maintaining procedures to ensure that proper handling of deposits and chargebacks is performed on a continuing basis; and
3. reconciling the bank account to the General Ledger cash account monthly.

D. CASHIERING STATIONS/MERCHANTS

Cashiers and Merchants are responsible for preparing the necessary deposit receipts and for ensuring that all Card transactions are submitted to CES with complete information, as set forth in the CES Operating Procedures Guide. In addition, they are responsible for sending spoiled or voided deposit receipts to their respective accounting officers.
VIII. REFERENCES

The Regents, Minutes discontinuing the requirement for specific Presidential approval by allowing the President to re-delegate the authority, January 1982.

President David S. Saxon, Memorandum to Vice President--Financial and Business Management on Delegation of Authority--Use of Commercial Credit Cards, February 25, 1982.

President J.W. Peltason, Memorandum to Senior Vice President--Business and Finance, Chancellors, and Laboratory Directors on Delegation of Authority--Use of Commercial Credit Cards, July 30, 1993.

The Regents' Bylaws, Section 21.4, on the Treasurer of the Regents authority to execute agreements in connection with banking related services.

Accounting Manual Chapter:
   C-173-14 Cash: Campus Cash Collection Deposits

Business and Finance Bulletin:
   BUS-49: Cashiering Responsibilities and Guidelines

Historical note: Original Accounting Manual chapter, Cash: Visa and MasterCard Commercial Credit Cards, first published 9/1/81; revised 6/1/82 and 4/1/87. Revision under the present title first published 3/31/95; analyst--Gayle Tapscott.