Cash Handling & Other Treasury Issues

CSU PDI 2010
January 8, 2010

Presented by Brian Grube, University Bursar
and Zach Campain, Bank Operations Specialist
Bursar’s Office Locations

- The Bursar’s Office is located in the Howes Street Business Center

- Cashiers Office is located on the main floor of the Lory Student Center next to The Flower Company (formerly the NORLARCO branch)
CASH Handling

When we talk about cash handling we mean more than dollar bills and change

- Coin and currency
- Checks (Personal, Traveler’s, Money Orders)
- Credit card transactions
Why is proper cash handling important?

- Protection of University Assets
  - Cash is a sensitive asset
  - Efficient handling ensures cash is protected, accurately processed, and properly reported in the University’s financial system.

- Protection of University Employees
  - Against inappropriate charges of mishandling funds
When would a department handle cash?

- Authorized Petty Cash Fund

- Sales of goods or services to the public
  - Receipt of Cash
  - Authorized Change Fund (or temporary cash advance)
Authoritative Guidance

- Colorado Revised Statutes
  - 24-36-103 – Transmit Monies to State Treasurer
  - 24-36-104 – Monies to be Deposited
  - 24-75-202 – Imprest Cash Accounts
  - 24-30-202(20.1) – State Controller Authority

- State Fiscal Rules - Chapter 6: Cash
CSU Guidance

- FPIs can be found on the Business & Financial Services web site
  
  http://busfin.colostate.edu/fpi.aspx

- FPI G-1 Petty cash / Change Funds

- FPI C-1 Receipt and Deposit of Cash, checks, and Credit Card Drafts
Petty Cash Funds
FPI G-1

- Used for purchasing small or emergency items or services (under $50)

- NOT for:
  - Payroll
  - To cash personal checks or make cash advances
  - Travel expenses (other than local mileage under $25)
  - Official functions
Petty Cash Funds
FPI G-1

- Request made with a “Request for a Petty Cash or Change Fund” form found on the B&FS web page under Forms and Treasury.
- Departmental personnel make purchases and request reimbursement from Petty Cash Fund custodian.
- Fund custodian requests reimbursement of fund through a KFS document with collected receipts from departmental personnel as back up.
- Fund should be reimbursed as often as necessary to ensure adequate availability for future purchases but at least once per month.
- Fund custodian should count (reconcile) the fund monthly or more often if needed based on transaction volume.
Change Funds / Temporary Cash Advance
FPI G-1

- Used for making change when goods or services are sold to the public.

- NOT for use as a petty cash fund. No purchases are to be made out of a change fund or temporary cash advance.
Change Funds / Temporary Cash Advance
FPI G-1

- **Change Funds**
  - Permanent – Cash is needed on an ongoing basis to support operations
  - Formal request process – Form found on B&FS website and requires Dean/Dept. Head signature

- **Temporary Cash Advance**
  - One time events – cash needs to be turned back into the Cashiers Office within 2 weeks.
  - Informal request process – email to Bursar’s Office detailing reason for the advance, dates needed, and breakdown of denominations
Sales to the Public
FPI C-1

- All sales should be recorded in a cash receipts log and pre-numbered receipts given to the customer.

- Checks should be IMMEDIATELY endorsed “For Deposit Only”

- Once a department receives receipts totaling $500 a deposit must be made to the Cashiers Office (and at a minimum once per month)
Best Practices in Cash Handling

Account for Cash as it is received

• If received in person, ring up on a cash register system or record on pre-numbered receipt form, giving a copy to the customer and retaining one for departmental records

• If received by mail or phone (credit card payments), record immediately on an order system, cash register, or cash receipt journal.

• Indicate the type of payment tendered on the record of payment
Account for Cash as it is received (cont’d)

- Ensure that checks are properly completed:
  - made payable to “Colorado State University”
  - are not stale dated or post dated
  - the numeric and written dollar amounts agree
  - it is drawn on a U.S. bank and payable in U.S. dollars
  - the check is signed by the payer.

- Look for counterfeit currency

  www.moneyfactory.gov
Best Practices in Cash Handling

- Separate Individual Cash Handling Duties

  • Separate the components of cash handling – collecting, depositing, and reconciling – so that one individual does not have responsibility for more than one component.

  • In small offices, this is not always possible, but separation of actual cash handling from reconciliation will help to deter fraud or concealment of errors.

  • Different employees should not work out of the same cash drawer. When responsibility for cash changes hands, it should be recorded with some receipting system.
Best Practices in Cash Handling

Safeguarding Cash

• Cash receipts and petty cash / change funds should be adequately secured at all times.

• Cash drawers should be locked when the employee responsible for it is away from his or her work station.

• At all other times, store coin, currency, and checks in a safe or locked secure place until they can be deposited at the Cashiers Office.

• Safe combinations should be changed whenever staffing changes occur among those that know the combination.
Best Practices in Cash Handling

Reconciling Activity

- Daily balancing should occur to reconcile the cash receipts register (cash register tape, pre-numbered receipts, or receipt log totals) to the Kuali deposit.
- Change fund should be counted to ensure it remains at the stated level.
- Any unidentified differences should be documented and a cash overage/shortage booked to the department’s operating account using object code 6634 (cash over & short).
Best Practices in Cash Handling

Monitoring the Cash Handling Process

Departmental administrators not directly involved in the cash handling process should periodically:

- Review the nature and extent of overages/shortages.
- Compare actual deposits recorded with expected receipts.
- Review activity reconciliations.
- Evaluate internal controls to ensure that adequate controls are in place to safeguard cash and that employees understand and follow the approved procedures.
Credit Card Best Practices
Credit Card Best Practices Education

- Examine the card!! Has it been altered in any way? Is it expired? Is it signed?
- Train employees on proper practices for accepting cards.
- Train employees on proper opening & closing procedures.
- Verify audit reports from POS device.
- Check signature with ID card.
- Perform AVS and CVV2 for CNP.
Credit Card Best Practices Education (cont’d)

- Storage of terminal sales receipts and reports – 18 months.
- Secured location – locked cabinet.
- Limited employee access – need to know basis.
- Terminal out of reach from customer.
- Truncation of sales receipts.
Common Merchant Mistakes

- Do not run your own card to fund the business.
- Never let another merchant or business use your account.
- Do not set minimum or maximum dollar $.
- Merchants are not allowed to add a usage fee to offset the cost.
- Do not split a trans into smaller amounts.
Fraud

- Economic impact
- Trusted employee
- Skimming
- Spoofing/Phishing
- Bank/Processor Fraud
- Cardholder Fraud
- Number Generators
- Stolen, Altered & Fake Cards
- ID Theft
Sensitive cardholder data

PCI DSS – Payment Card Industry Data Security Standards
- A set of comprehensive requirements for enhancing payment account data security.
- Security standard established to proactively protect customer account data.

<table>
<thead>
<tr>
<th>Technical Guidelines for PCI Data Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Element</td>
</tr>
<tr>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Cardholder Data</td>
</tr>
<tr>
<td>Primary Account Number (PAN)</td>
</tr>
<tr>
<td>Cardholder Name</td>
</tr>
<tr>
<td>Service Code</td>
</tr>
<tr>
<td>Expiration Date</td>
</tr>
<tr>
<td>Sensitive Authentication Data</td>
</tr>
<tr>
<td>Full Magnetic Stripe Data</td>
</tr>
<tr>
<td>CAV2/CVC2/CV2/CID</td>
</tr>
<tr>
<td>PIN/PIN Block</td>
</tr>
</tbody>
</table>
Sensitive cardholder data

PCI DSS – Payment Card Industry Data Security Standards
Questions?
Comments?
Feed Back