AUDIT AND ADVISORY SERVICES

Assess Improve Monitor

AIM higher

ISSUE #5—MAY 2017

INSIDE THIS ISSUE

KEY POLICIES

- UC Policies (policy.ucop.edu)
  - UC Accounting Manual
  - UC BFB-BUS-49—Cash and Cash Equivalents
  - UC BFB-G-41 Employee Non-Cash Awards and Other Gifts
- UCSF Policies (policies.ucsf.edu)
  - Cashiering 300-14
  - Petty Cash and Change Funds 300-44

IMPLEMENTING EFFECTIVE FINANCIAL CONTROLS

While effective financial management is made up of many components, below are ten steps department managers can take to institute controls over their finances and manage risks:

- Document and maintain policies and procedures so that they are easily accessible to department employees requiring that information
- Maintain effective separation of duties to ensure that no one person performs more than one of the following steps:
  - initiates a transaction
  - approves the transaction
  - records the transaction
  - reconciles balances
  - handles assets
  - prepares or review budget status reports
- Physically safeguard assets (equipment, supplies, cash, and other assets) against unauthorized access, use, disposition, or loss
- Conduct periodic counts or physical inventories and compare amounts on hand to system or control records
- Maintain proficiency with cash handling requirements by taking "UCSF Cash Policy Highlights" via the UC Learning Center (this is an annual requirement for Cash Handlers and Depositors)
- Secure information systems with strong passwords for critical accounts as well as encryption of physical devices and back-ups of critical data
- Submit and approve expense reimbursement requests no later than 45 days after the completion of a trip or event (to avoid the possibility of having the expense reported as taxable income to the individual being reimbursed)
- Review Business and Finance Bulletin 79 (BUS-79) Expenditures for Entertainment, Business Meetings, and Other Occasions for allowability and expenditure limits
- Conduct ledger reviews regularly, monitor allowable costs for sponsored activities, and minimize late cost transfers
- If an exception occurs, ensure that the Late Cost Transfer Policy Exception Request Form includes the required explanation and supporting documentation to justify the transfer

For additional information, review the available training and job aids on the UCSF Controller's Office website at **http://controller.ucsf.edu**.

MEET OUR TEAM

Bryan came to UCSF from the Texas State Auditor's Office in Austin. Prior to that, he worked at the Texas Department of Public Safety Crime Lab as a Digital Evidence Examiner. Originally from New York, Bryan has an MBA and MSc (High Technology Crime Investigation) and has obtained the Certified Fraud Examiner (CFE) credential.

1855 Folsom Street
Suite 107
San Francisco, CA 94143
Phone: (415) 476-3851

If you have any questions, or need advice or assistance with emerging risk or internal control issues, you can contact us at:
AuditAdvisor@ucsf.edu
http://audit.ucsf.edu

UC Whistleblower website and Hotline:
http://ucwhistleblower.ucop.edu
(800) 403-4744

UCSF

FRAUD CORNER

University of Alabama Hospital Employee charged with stealing $1.1M in cash over 9 years

A financial account representative at the University of Alabama at Birmingham's Hospital Food and Nutrition Services Department whose job it was to make change for cashiers in the hospital dining areas was sentenced to 18 months in prison after she pleaded guilty to stealing $1.1 million in cash. She admitted to the FBI that she began taking cash from the cash room in 2008 – usually taking no more than $900 at a time.

Lawyer sentenced to prison for stealing $1.2M in patient payments

Mr. Gallas' firm, Gallas & Schultz, collected past-due payments from patients for the hospital network. Money collected by the firm on behalf of St. Luke's was supposed to go into a trust account. However, Mr. Gallas admitted that he had employees put holds on more than $1.2 million in collections and transfer the funds to the law firm's operating account.

Anti-Fraud Strategy: Background Checks

"I'm sorry Sir, but your background check has bounced."

http://onboardingspecialties.blogspot.com/2015/07/background-checks-are-they-necessary.html

In addition to implementing physical safeguards over cash itself, one of the most important controls in fraud prevention is ensuring that all employees with cash handling duties receive an effective pre-employment background check. These checks can reveal a potential employee's experience with cash handling as well as any personal financial history that may impact future job duties and performance.

DID YOU KNOW…?

UCSF Policy 300-14 requires that employees with cash handling responsibilities who are convicted of any crime while employed by UCSF must report that conviction to Risk Management Services and the UCSF Police Department.

CASH HANDLING REQUIREMENTS

As the most liquid of assets, cash must be constantly protected against loss. UC BFB-BUS-49—Cash and Cash Equivalents provides guidance and best practices for handling cash and cash equivalents at campus locations; noting that accountability, separation of duties, physical security, and reconciliations are key components of a successful cash control strategy. Some best practices in these areas include:

- Keeping cash stored securely; for example:
  - ◊ Each person responsible for handling cash should have their own individual cash drawer with unique identifiers to distinguish it from others
  - ◊ Funds needed during the day should be kept in a locked, controlled area and stored overnight in a safe
- Confirming cash balances both before and after each work day
- Recording cash as soon as it is received and providing receipts for all payments
- Immediately upon receipt endorsing all checks as "For Deposit Only"
- Ensuring an effective separation of duties so that the same person does not receive and prepare the deposit for cash
- Voided or credit transactions should be reviewed and approved by a supervisor
- Deposits should be verified by a supervisor
- Reconciliation of bank statements to deposit slips should be done by personnel not associated with preparing the deposit
- If any losses occur, they should be reported to a supervisor as soon as they are identified
- Cash handling training should be provided to all employees who handle cash immediately upon hire and at least once per year thereafter

https://s-media-cache-ak0.pinimg.com/564x/aa/74/d5/aa74d5e3c754dfefd4a3e196f8df05a0.jpg

TO GIFT OR NOT TO GIFT

The focus is often on cash or checks when protecting against theft; however, there are many cash equivalents such as gift cards or vouchers that are also at risk for theft and improper use and require proper safeguards and controls. Some key controls that should be considered for these non-cash items include:

- Policies and Procedures—documents that outline the procedures for the administration, distribution and use of gift cards/vouchers
- Pre-numbering of vouchers—identifiers that allow for accountability of the cards/vouchers
- Tracking and monitoring—a log recording transactions of cards/vouchers received, issued, and on-hand
- Secure storage—a locked cabinet or safe that restricts access to the cards/vouchers to authorized personnel
- Reconciliation—periodic comparison between the log records and the quantity of cards/vouchers on hand
- Segregation of duties—different individuals maintaining custody of the cards/vouchers and reconciling their use

PCI COMPLIANCE

When transitioning from collecting cash to processing credit card transactions, the risk focus shifts from receiving and protecting revenue to receiving and protecting data. The Payment Card Industry (PCI) has come up with a set of Data Security Standards (DSS), which outline how to handle, store, and secure credit card data.

UCSF has a group dedicated to ensuring compliance with PCI DSS, but there are things that everyone can do to help, such as:

- Never e-mail credit card information or store credit card numbers in any database or spreadsheet. Truncate all but the last four digits of the card number.
- Keep all credit card documentation locked.
- Destroy credit card documentation when no longer needed.
- Limit access to cardholder information to only those employees with a legitimate need to know.
- Segregate duties so that the person performing reconciliation isn't involved in processing credit card sales or refunds.

Additionally, if you are looking into accepting credit card payments or changing the current method of accepting payments, contact the PCI workgroup at askPCI@ucsf.edu to make sure that UCSF is accepting payments correctly. Many different groups may affect the PCI DSS compliance at UCSF, including web-hosting companies, payment gateways, marketing firms, and credit card machine maintenance providers, and contracts need to be in place to ensure that these groups are not putting UCSF at risk.