

An aerial photograph of the University of California campus, showing various buildings and greenery. In the background, the San Francisco skyline is visible through a light haze. The text is overlaid on the upper portion of the image.

University of California
2019 Ethics, Compliance and Audit
Symposium

REACHING NEW HEIGHTS

Red Flag Fraud Indicators

Niloufar Alian – UCR Audit and Advisory Services, Principal Auditor

Janet Cox – UC Davis Audit & Management Advisory Services, Principal Auditor

Tony Firpo – UC Davis Audit & Management Advisory Services, Associate Director

Jean Lee – UCLA Audit & Advisory Services, Audit Manager

Pamela Magana-Britton - UCLA Audit & Advisory Services, Audit Manager

Agenda

- ❖ Travel Fraud Analytics – Tony Firpo and Janet Cox (UC Davis)
- ❖ Cash – Jean Lee (UCLA)
- ❖ Purchasing – Pamela Magana-Britton (UCLA)
- ❖ Fraudulent Vendor Billing Scheme – Niloufar Alien (UC Riverside)



TRAVEL FRAUD ANALYTICS

Janet Cox, Principal Auditor, UC Davis

Tony Firpo, Associate Director, UC Davis

Travel Fraud

The Association of Certified Fraud Examiners reports

- Expense reimbursement fraud counts for 11% of fraud in large organizations
- Travel fraud is often considered easy to detect, if you are looking for it
- Can be an indicator of other/larger problems. If someone is willing to perpetrate one type of scheme, they are likely willing to perpetrate others
- Pink collar crime is on the rise

Identification of Fraud



- Original issue was the result of a whistleblower complaint
- Using ACL, identified all current staff with the same title code
- Trend and comparison of expenses by type
- Summarized by mileage, lodging, meals, entertainment and morale
 - Excluded group travel, recruitment and relocation expenses
- Identified the highest spend employee in each category for comparison to whistleblower concern.

This identified additional employees with potential concerns so further analysis was performed

Data Analytics

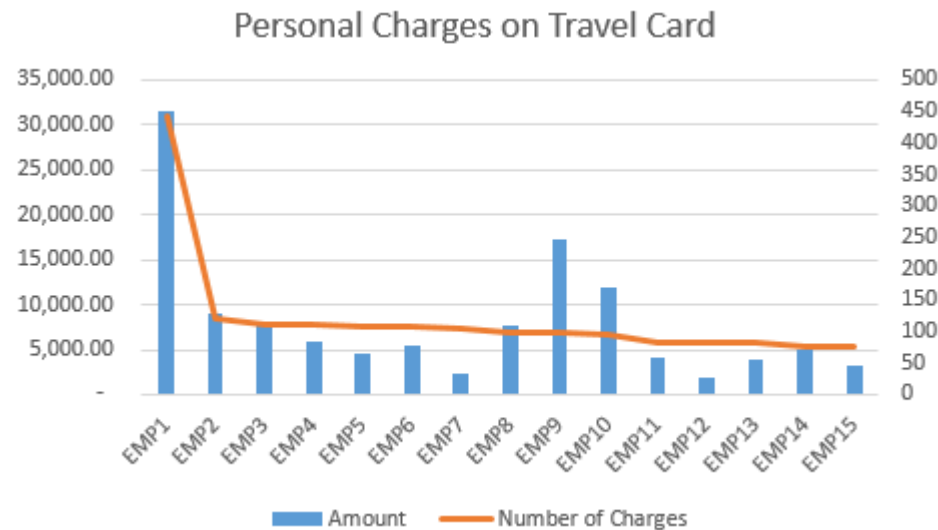
Data used:

- Concur report table to add report header details (i.e. report name, travel dates)
- Concur report entry tables - show individual transactions
- Concur audit log table
- Eventually, access to view individual reports by employee in Concur
- US Bank Visa account information

Individual traveler credit card statements

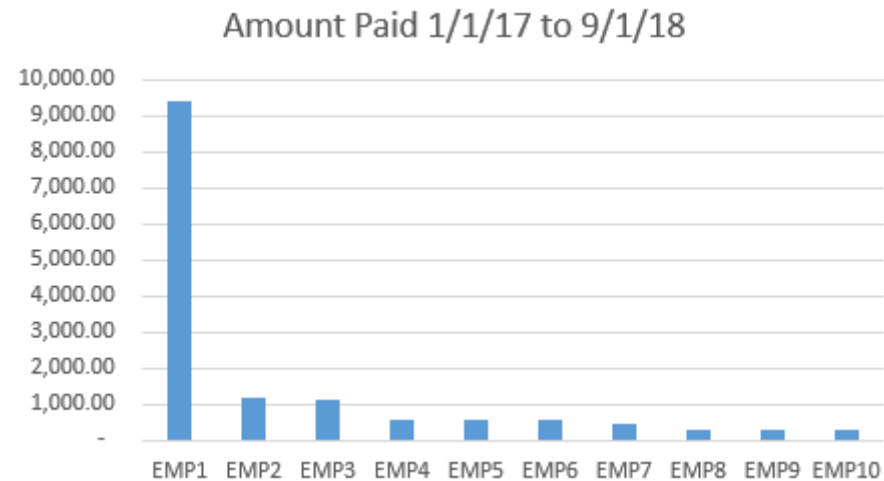
Data Analytics Testing

- Personal transactions charged to corporate travel card (identified by traveler)
 - Report Entry - Is_Personal =Y



Data Analytics Testing

- Excessive Mileage
 - A comparison of mileage reimbursement for specific title code, Administrative Officers



Data Analytics Testing

Tests performed

- Cash advances obtained via an ATM vs a teller inside the bank

MCC_Code = 6010 (teller) or 6011 (ATM)

- Starbucks reloads

Merchant Name = "Starbucks" / Merchant City = 800-782-7282 / MCC code = 5499 (Misc food stores, vs. the more common 5814- fast food restaurants)

- Split transactions

Transactions on the same card and on the same day with both transactions being less than \$75.

- Frequent credit transactions on the travel card

A credit transaction will impact the balance the same as a payment

Data Analytics Testing ctnd...

- Duplicate payments

Payments to an employee for the same dollar amount/transaction and the same date

- Transactions on weekends and/or UC Holidays

- Unusual activity with specific vendors

Entertainment meals purchased at TJ Maxx; meeting supplies from Home Depot

- Did the department approver view the supporting documentation?

Travel Report Analytics

- Isolated expenses

Airfare or Lodging with no related business expenses. Like meals, mileage or rental car

- Overlapping trips

Traveler with lodging/airfare in another location for specific dates but travel card was used locally during that time frame

- Reports with vague or unsupported business purpose

Considering results of other data analysis

Travel Report Analytics

- Invoices with inconsistent tax rates or that don't foot

Total cash rate	2,160.00
Destination Amenity Fee	150.00
Estimated government taxes and fees	190.00
Total for stay in hotel's currency	2,500.00 USD

Total cash rate	2,032.00
Destination Amenity Fee	150.00
Estimated government taxes and fees	318.00
Total for stay in hotel's currency	2,500.00 USD

Order Placed: January 24, 2019
 Amazon.com order number: 113-1206622
 Order Total: \$89.97

Shipped on January 25, 2019	
Items Ordered	Price
3 of:	\$29.99
Sold by: American Closeouts (seller profile) Condition: New	
Shipping Address:	
United States	
Shipping Speed:	
Two-Day Shipping	

Payment information	
Payment Method:	Item(s) Subtotal: \$81.52
Visa Last digits:	Shipping & Handling: \$0.00
Billing address	-----
	Total before tax: \$81.52
	Estimated tax to be collected: \$0.00

	Grand Total: \$89.97

Travel Report Analytics


- Documents with headers/footers that don't match the body of the document

STAY DATES

Fri May 03, 2019 -
Sat May 11, 2019

Room(s): 1

Adult(s): 1

 **JW Marriott** [redacted]
[redacted] USA
Phone: [redacted] 0300

#98862245

[redacted] thank you for your reservation. The required deposit has been charged to your card. An email with this information has been sent to [redacted]. We look forward to greeting you soon.

As of December 2017, your receipt for hotel stays in the U.S. and Canada may be automatically sent to you at the email address above. If you prefer, a paper copy may be requested at the front desk when you check in. [Learn how to change your email address.](#)

Summary of Charges (USD)

Room Type: 1 Bedroom, King
[redacted]

<https://www.marriott.com/reservation/findReservationDetail.mi?confirmationNumber=98974269&tripid=98974269&propertyId:>

Travel Report Analytics

- Verification of hotel or airline confirmations showed the reservation was cancelled or changed

138598890054

Hotels.com Confirmation Number: 138598890054
Booked: Online - Wednesday, May 31, 2017 8:38:12 PM PDT

Your Receipt

Billing Name: University of California, Davis
Company details:
University of California, Davis
One Shield Avenue
Davis, CA 95616
USA

Booking Details

Guest Name:	Room Type:	Standard Room
Check-in:	Hotel Details:	Aqua Ohia Waikiki
Check-out:		2280 Kuaio Ave
Number of Nights: 5		Honolulu
Number of Rooms: 1		US
		+18089286442

Charges: USD \$

Monday, June 5, 2017:	\$149.09
Tuesday, June 6, 2017:	\$139.08
Wednesday, June 7, 2017:	\$139.08
Thursday, June 8, 2017:	\$139.08
Friday, June 9, 2017:	\$149.09
Discount applied:	\$0.00
Sub-total:	\$715.42
Tax recovery charges and service fees:	\$99.90
Total Price:	\$815.32
Amount paid:	\$815.32
Amount still due:	\$0.00
Additional fees charged by the hotel:	\$90.00
Total cost for this booking:	\$905.32
Payment Method:	Visa
Card number:	

Cancellation Policy
Free cancellation until 06/02/17

Confirmation number	138598890054
Check-in	Monday, June 5, 2017
Check-out	Saturday, June 10, 2017
Your stay	Cancelled
Total amount	\$0.00
Room details	
Your room	Cancelled

What's Next?

- Implement a data analytics program to review and trend travel and entertainment expenses monthly
- Update training materials for those approving travel and entertainment documents with clarification of requirements to support the business purpose
- Additional approvals for business managers travel and entertainment reports
- Development of an escalation protocol to address concerns identified
- Expanded monthly spot audits
- Develop tools to educate community on fraud and fraud prevention



CASH

Jean Lee, Audit Manager, UCLA

CASH – Voids and Refunds

- ❖ Data Analytics - Trends of Voids/Refunds
 - “Patient left without being seen.”
 - “No-show.”
- ❖ Verified the Data - Medical Records
- ❖ Employee – Trusted, Rarely Took Vacation
- ❖ Corrective Action:
 - Trend Data
 - Periodic Management Review
 - Spot Checks

VOID

Cash – Petty Cash Fund (Swag Sales)

Swag Sales funded the Petty Cash Fund for one department.

- ❖ Discovered through questionnaires and physical observation.
- ❖ No receipts were given.
- ❖ Only cash was accepted.
- ❖ Sales were not recorded.
- ❖ Sale proceeds (cash) were handed to an individual, who stored funds in the petty cash fund in her office.
- ❖ No deposits were ever made to the bank.



Cash – Petty Cash Fund (Swag Sales)

- ❖ No Reconciliations.
- ❖ No Oversight.
- ❖ No Cash Counts.
- ❖ Employees were told to “Be Honest,” honor system.
- ❖ Corrective Action: End swag sales and discontinue the off the books petty cash fund.



Cash – Petty Cash Fund (Printing Fees)

- ❖ Printing Services & Fees
- ❖ Discovered through interviews and physical observation.
- ❖ No deposits to the bank (bank statements). Money was kept “off the books.”
- ❖ No receipts.
- ❖ No separation of duties.
- ❖ Lack of accountability.
- ❖ Corrective Action: Twice each day, one of the front desk staff will take the money in the locked box downstairs to the Fiscal Officer’s office. The student intern will count the money, along with the receiving Fiscal Officer. Monies are then stored overnight in this office, with limited access to one individual. Monies will be regularly deposited and an independent person will reconcile deposits to the general ledgers and bank statements.

Cash – Key Deposits



❖ Two cases:

- 1) Discovered because an employee went on leave and staff found safe with cash and over a hundred checks. The employee rarely took vacation.
- 2) Through interviews, observations, and a surprise count.

❖ There was \$1,500 in the petty cash fund box, including four \$100 bills. It was unclear who accessed the funds and made change or took funds from the box.

Cash – Key Deposits



- ❖ Accountability was not maintained.
 - The key to the box was stored in an unlocked drawer in the office.
 - The locked box was stored in an unlocked drawer in the office.
 - Multiple people had access to the funds.
- ❖ No deposits made.
- ❖ No reconciliations or oversight.
- ❖ No surprise counts.
- ❖ No receipts, no records.

Cash – Key Deposits



Corrective Action:

- ❖ Numerically sequenced receipts.
- ❖ Key log – online database to track.
- ❖ Use of the student billing system to eliminate use of cash as much as possible.

Cash – Corporate Cards

- ❖ Discovered through sample testing and reviewing transactions.
- ❖ “Gut Instinct”
- ❖ Other Indicators (Staff Morale)
- ❖ Unusual charges in the sample testing review.
- ❖ AOL Internet Charges
- ❖ Spa Treatments
- ❖ Chocolates
- ❖ Resulting Action – Employee was let go. New leadership.





PURCHASING

Pamela Magana-Britton, Audit Manager, UCLA

Purchasing

- The fraud
- Investigation
- Factors that contributed to the fraud occurring
- How to help prevent this type of fraud
- Takeaways for auditors

The fraud

- Who discovered the fraud – The new Chief Administrative Office (CAO)
- Who committed the fraud – Trusted, long time employee
- How long was it going on – 10 months



Investigation

- Financial System Reports
- Accounts Payable System
- Purchase Orders (PO)
- Store Receipts
- Data Analytics
- Security Camera Footage
- Emails
- Interviews



Factors that contributed to the fraud occurring

- Lack of an appropriate structure for handling the department's financial resources
- No separation of duties
- Trusted employee
- No one was monitoring or evaluating financial data
- Student Store personnel were not following standard pick up procedures



Controls to help prevent this type of fraud from occurring

- ✓ Proper training of financial systems
- ✓ Separation of duties
- ✓ Fiscal oversight
- ✓ Financial reconciliations
- ✓ Reviewing purchasing transactions
- ✓ Monitoring and evaluating financial data
- ✓ Following policies and procedures





FRAUDULENT VENDOR BILLING SCHEME

Niloufar Alian, Principal Auditor, UC Riverside

Fraudulent Vendor Billing Scheme

Case: An allegation was made by an XYZ University employee regarding a possible fictitious vendor billing scheme.

How this case was first discovered

An XYZ University Supervisor, while performing reconciliation procedures, found that vendor statements received from LG Company did not reconcile to the payments made to this particular vendor. Specifically:

- The Supervisor suspected the possibility of a fraudulent check totaling \$5,500 to LG Company.
- There were two invoices from LG Company in one month with different amounts. It appeared that this vendor was paid twice in one month.
- The Supervisor indicated that he did not stamp “Ok to Pay” on the invoice and it appeared that the “Ok to Pay” was photocopied from another invoice.
- The Supervisor contacted LG Company to confirm the payment but the vendor was not able to identify the payment (totaling \$5,500) that was supposedly made to them.
- This case was immediately reported to the appropriate authority and was brought to XYZ University Internal Audit’s attention.

XYZ Auditors searched for possible additional fraudulent payments through Data Analytics:

Methodology:

- a) Auditors ran a PeopleSoft Financial Query Report choosing Payment Table.
- b) Scope: FY 2010 to FY 2019 (all payments to all companies)
- c) From the Payment Table, the auditors selected Vendor ID, Vendor Name, Check Number, Month, Amount, Addresses
- d) Exported the results to Excel for further analysis and verification purposes. (see next slide)

Analysis 1 Different Addresses, Same Vendor

Vendor ID	Vendor Name	Check #	Month	Check Amount	Addresses
12356	LG	101	January	2500	123 Main Street
12356	LG	102	February	3000	123 Main Street
12356	LG	111	February	5500	3434 Central Ave

Objective:

The objective of this analysis was to determine if the allegation by XYZ University Supervisor is substantiated based on the preponderance of evidence standard.

Results:

Auditors created a filter to extract payments for LG Company. The Auditors were able to verify that there was a duplicate payment in the month of February made to this Company under different a address.

Analysis 2

Same Addresses , Different Vendors

Vendor ID	Vendor Name	Check #	Month	Check Amount	Addresses
12356	LG	101	January	\$ 2500	123 Main Street
12356	LG	102	February	\$ 3000	123 Main Street
12356	LG	111	February	\$ 5500	3434 Central Ave
56748	ATT	115	March	\$1500	456 Market
56748	ATT	201	March	17,402	3434 Central Ave
88997	YM	102	June	2500	666 Riverside Ave
88997	YM	103	July	2500	666 Riverside Ave
88997	YM	104	July	10,000	3434 Central Ave

Objective:

The objective was to determine if different vendors were getting paid under the same address and this address was accurate.

Result:

Auditors created a filter to extract payments for other companies (including LG). The Auditors found that the same address used for Company LG was also used for Companies ATT and YM. Based on this analysis, auditors determined that Companies ATT and YM had also duplicate payments in one month totaling \$27,402. These checks were identified by Auditors.

Management Attention

The Auditors brought up these issues to XYZ University management's attention immediately after they were identified. XYZ University management took action as noted below:

- Reviewed the bank statements and obtained check images to determine if these checks were cashed.
- Put a stop on the check made to the Company ATT for \$17,402 since it has not been cashed yet.
- Conducted additional research to find out why this check was not cashed, and found that the bank has a control in place (Positive Pay). This control prevents the check from being cashed if the address does not match to the address in their system.

Verification

Objective: To determine if the Company is legitimate.

The Auditors compared the addresses in Google Map:

LG Address A

LG Address B

Results:

The picture on the left below showed that the address 123 Main Street is the correct address of LG Company.



Verification Vendor Master File

Summary | Identifying Information | Address | Contacts

SetID: XYZ
Vendor ID: 12356
Vendor Short Name: [REDACTED]
Vendor Name: [REDACTED]
Order: [REDACTED]

Status: Approved
Persistence: Regular
Classification: [REDACTED]
HCM Class: [REDACTED]
Open for Ordering: Yes
Withholding: No
VAT: No

Remit To: [REDACTED]

Last Modified By: Joe Bruin
Last modified date: 07/30/2019 12:00AM
Created By: [REDACTED]
Created Datetime: [REDACTED]
Last Activity Date: [REDACTED]

Save | Return to Search | Notify | Refresh | Update/Display | Correct History

Summary | Identifying Information | Address | Contacts

Objective:

Auditors reviewed information regarding Company LG in the Vendor Master File to determine if the address was changed and who changed the address in the Vendor Master File System.

Results:

Based on the review, the Auditors were able to identify the individual who modified the Vendor Master File. However, they were not able to determine what information had been changed in the Vendor Master File. The second address HAD to be added then it was deleted with a correction mode. Auditors were not able to investigate further because the audit trail functionality was not implemented.

Verification

Vendor Master File

- Auditors obtained individual access status in Vendor Master file from Technology Services (ITS). Auditors reviewed each individual's access and related information and determined that some individuals who had access to invoices, had also read/write access to Vendor Master Files. (lack of segregation of duties)
- Auditors also determined that there is no adequate control in place to review the vendor master file periodically and determine if changes to addresses and vendors are appropriate.

Verification Purchase Order FAT Purchase Order (opportunity)

Auditors expanded their investigation procedures by:

- Reviewed Company LG information in the Purchase Order System (eBuy).
- Found that Company LG was set up as a blanket purchase order totaling \$100,000.
- Since the amount of payment did not exceed \$100,000; the system was not able to put a stop on the fraudulent payments.

Verification

Invoice Comparison and Image Checks Review

The Auditors reviewed the fraudulent invoice and related check image for LG Company and compared these to the original invoice from the same Company and noted the following:

- Remit to/Invoice Date/Invoice Number appeared to have been modified (Different Font)
- The Due Date was poorly aligned
- The Fraudster “fat fingered” the fake remit address
- The Image check was not endorsed but cashed (see Check Image Slide)
- The Invoice used an old format as a new format was already being used starting February
- The Due date was not modified to reflect the date of the invoice
- Even the fraudulent address was typed wrong compared to other fraudulent invoices

Control Weakness Identification

- Lack of adequate segregation of duties
 1. Employees who processes checks and can enter invoices
 2. Employees who audits checks against the backup documentation, notes discrepancies can also enter invoices
- Lack of adequate/periodic review of the individual's access to the vendor master file
 - The Vendor Master File could easily be altered by various employees
- Lack of adequate or periodic review of invoices and payments by various departments to ensure payments are received timely and appropriately by a proper vendor
- Invoices were mailed directly to the different departments instead of the Central Accounting unit

Communication

These issues were communicated with appropriate management at XYZ University by internal auditors. Some corrective action plans have been already been implemented by management.

Recommendations

- A proper segregation of duties for individuals with access to change the Vendor Master file to ensure that the ones who can make changes to the vendor master file would not have the ability to handle or enter invoices.
- Review access to the Vendor Master File periodically.
- Restrict authorized access to the Vendor Master File.
- Review invoices and payments monthly to ensure that payments are made to proper vendors.
- Contact vendors frequently to ensure that payments are received appropriately and timely.
- Review vendor master file on a consistent bases.

Questions?



Contact Information

Niloufar Alian – UCR Audit and Advisory Services, Principal Auditor

niloufar.alian@ucr.edu

Janet Cox – UC Davis Audit & Management Advisory Services, Principal Auditor

jmcox@ucdavis.edu

Tony Firpo – UC Davis Audit & Management Advisory Services, Associate Director

affirpo@ucdavis.edu

Jean Lee – UCLA Audit & Advisory Services, Audit Manager

jlee@iad.ucla.edu

Pamela Magana-Britton - UCLA Audit & Advisory Services, Audit Manager

maganabritton@iad.ucla.edu