Fighting Financial Fraud

February 11, 2019

Sandy Sturgeon, Director of Financial & Management Analysis
sandras@uark.edu; 575-5553
Today’s Agenda

- Fraud Defined
- How Do We Rank?
- Common Fraud Scenarios in Education
- Who Commits Fraud?
- Red Flags
- Tests
- Internal Controls
- Fraud Landscape – We Are Not Alone
**Fraud Defined**

*Fraud* has many definitions but at its core it is something said or done in a dishonest way in order to trick people out of their rights or property.

*Fraud* can be a civil matter, a criminal matter, or both:
- a criminal offense by prosecutors or a civil action by the victim.
What is Occupational Fraud?

*Occupational Fraud* is fraud committed by an employee on an employer in the course of their employment.
What is Occupational Fraud?

There are three major types of Occupational Fraud:

1. Corruption
2. Asset Misappropriation (today’s focus)
   - Fraudulent Disbursements
3. Financial Statement Fraud
The Fraud Tree

THE FRAUD TREE
OCCUPATIONAL FRAUD AND ABUSE CLASSIFICATION SYSTEM

Corruption
- Conflicts of Interest
- Bribery
- Illegal Gratuities
- Economic Extortion

Asset Misappropriation
- Embezzlement
- Misuse of Entities
- Theft

Financial Statement Fraud
- Misrepresentation
- Falsification
- Erasure
- Other

Inventory and All Other Assets
- Misrepresentation
- Falsification
- Erasure
- Other

Theft of Cash
- Theft of Cash on Hand
- Theft of Cash from Petty Cash

Fraudulent Disbursements
- Filing of False Claims
- Altered Documents
- Other

Monies
- Theft of Monies
- Theft of Cash on Hand
- Other

Fraud effects almost every industry, including Education.

Among the occupational industries at risk of fraud and abuse, Education ranked 6th among 15 industries surveyed for the number of reported fraud cases. Banking & financial services was #1.

Yet, the Education sector had the 2nd smallest reported median loss of $68,000 (just behind retail which reported a $50,000 median fraud loss).

Fraud in Education outranked many other industries, including insurance, professional services, transportation, construction and religious/charitable or social services.

Across all 15 industries surveyed fraud was primarily detected through anonymous employee tips, management review, and internal audit.
The 2018 ACFE report identified the following as the highest areas of fraud in the Education sector:

- 38% Corruption
- 23% Billing Fraud
- 19% Cash Larceny
- 19% Cash-on-hand Fraud
- 19% Non-cash Fraud
- 18% Expense Reimbursements
- 14% Skimming
Common Fraud Scenarios in Education

- Conflicts of Interest
  - Admissions
  - Hiring
- Purchasing:
  - Bribery
  - Incentives/Kickbacks
- Personal Purchases on a University P-Card
- Forgery of University documents
Common Fraud Scenarios in Education cont’d

- Theft of Cash from Deposits
- Misappropriation, Misuse or Theft of University Property or Equipment
- Payroll and Overtime Fraud
  - Falsification of timesheets to over-report hours
- Expense Reimbursements
  - Fictitious or Over-Claiming of Expenses
Most Common Reason Fraud Occurs

- **One person** is given **complete control** of a financial process from beginning to end without any oversight or monitoring from a supervisor or Department head.
Weaknesses That Contribute to Fraud

- Lack of internal controls: 30%
- Override of existing controls: 19%
- Lack of management review: 18%
- Poor tone at the top: 10%
- Lack of competent personnel in oversight roles: 8%
- Other: 6%

- Lack of independent checks/audits: 4%
- Lack of employee fraud education: 2%
- Lack of clear lines of authority: 2%
- Lack of reporting mechanism: <1%
Who Commits Fraud?
Demographic of Fraudsters within An Organization

- Peak age range was 36 – 45 (mid career)
- Males were reported to commit 69% of fraud compared to females 31%
- 47% of fraudsters had a University degree
- Only 4% of fraudsters had a prior fraud conviction
- #1 Behavioral Red Flag Displayed by Fraudsters? Living Beyond Their Means (41% of all reported cases)
Those with 1-5 years of tenure commit 44% of reported fraud. Prior to 2010 this was not the case.

WHAT HAS CHANGED?

- Millenial differences — invincible, deserving, seek instant gratification, frequently change jobs, less employer loyalty, not defined by their jobs
Payroll schemes tend to last the longest, with a median duration of 30 months until discovery, while schemes involving cash on hand and register disbursements were both typically uncovered one year after they began.
How Do I Get A Copy of the ACFE Report?

If you want a copy of the 2018 Report to the Nations it can be found at:

https://www.acfe.com/report-to-the-nations/2018
The Fraud Triangle

Rationalization
Justification of dishonest actions.

Stupid people deserve to be cheated. They had it coming. If we did not do it someone else would have. They need our leadership.

Opaque and unnecessarily complicated systems involving rigged transactions, naïve and trusting public, and weak regulators. Privileged connections, positions of trust, access to people's money.

FRAUD

Insatiable greed and lust for power with little balance from moral principles and human empathy.

Opportunity
Ability to carry out misappropriation of cash or organizational assets.

Pressure
Motivation or incentive to commit fraud.
Red Flags

Individually a red flag doesn’t mean there is a fraud occurring, but it does mean we should be on alert & mindful
Red Flags Won’t All Be This Obvious
Most Common Fraudulent Disbursements

- Billing Schemes
  - Shell Company
  - Non-Accomplice Vendor
  - Personal Purchases

- Payroll Schemes
  - Ghost Employee
  - Falsified Wages
  - Commission Schemes

- Expense Reimbursement Schemes
  - Mischaracterized Expenses
  - Overstated Expenses
  - Fictitious Expenses
  - Multiple Reimbursements

- Check Tampering
  - Forged Maker
  - Forged Endorsement
  - Altered Payee
  - Authorized Maker

- Register Disbursements
  - False Voids
  - False Refunds
What to Look For in People

- Over-concerned or over-interested in particular contracts or vendor payments
- Prefer to work outside of normal business hours (e.g., weekends, evenings, holidays)
- Try to “rush” the procurement or payables processes and typically only provide requested information after multiple requests and an unreasonable time delay
- Strong desire to remain the sole source of contact between a particular vendor & the University (control issues – doesn’t want to share duties or information about a contract or vendor)
- Appears to have social relationships with suppliers (e.g., vendor sponsored golf outings, tailgate parties)
- Lifestyle don’t match salary or a lifestyle that suddenly increases with no apparent reason (e.g., big lottery win, inheritance)
- Frequent talk of severe financial issues or high personal debts.
- Model employees – they never take vacations, always come in early and stay late
What to Look For in Documents

- Missing documents – multiple “Lost Receipt” forms, lack of basic vendor information, missing phone numbers, photocopies, faxes, or scanned documents provided as support
- Obvious alterations or discrepancies in provided documentation
- Handwrittten documents
- P.O. Box or Mail Drop addresses with no apparent physical address aren’t as much of a red flag as they used to be – UPS Store & Post Office customers have real street addresses now
- Pattern of invoices slightly below bid limits
- Initial low bids awarded, however, followed up with multiple change orders
- A losing bidder who is hired by a winning bidder - which may suggest that the winning bidder was not adequately qualified to perform the work
What to Look For in Documents cont’d

- Invoices provided as documentation that do not appear to have envelope fold marks
- Address of employee is same as the vendor
- Duplicate payments
- Round Dollar Amount Invoices
- Vendors with a High Number of Cancelled or Returned Checks
- Odd, unusual or different transactions (items purchased that do not align with vendor – e.g. landscaping supplies purchased from an office supply store)
ACH Payment Instruction Changes

- Examine the Physical Check
  - Look at the edges – are they perforated or rough edge? Are all the sides smooth?
  - How big is the check? Personal checks are the size of US paper currency - Business checks tend to be larger ledger size
- Check the Bank Logo & Address
  - A quick Google search should return the bank’s website and its legitimate logo and address
- Examine the MICR Line
  - Is the Routing Number, Account Number and Check Number in the correct sequence?
  - Does the check number agree?
  - Go to the Federal Reserve Bank Services website and search the routing #; does the bank information agree to the physical check? Where is the bank located? [www.frbservices.org](http://www.frbservices.org)
ACH Payment Instruction Changes cont’d
Look for the American Bankers Association (ABA) number generally in the upper right hand corner. It’s a fraction such as 12-34567/8901 which represents bank, location, and Fed branch servicing bank.

Is the Padlock Icon present? The small padlock symbol which is a registered mark of the Check Payment Systems Association indicates additional security features have been incorporated into a check’s design, production and materials.

Feel the paper – is it sturdy check stock? Does the color easily smear?

Check for irregularities

- Check for spelling or typing errors within any of the printed areas
- Are there odd abbreviations?
- Is the check a personal or business check

Scammers often communicate with their victims using poor grammar/spelling or vague language - look closely at all emails or communications received.
Phishing Schemes in the AP Environment

- Looks like legitimate correspondence from a vendor – **BUT** ……
- asks that you click on a link to obtain a form, further information, or updated contact/account info.
- Contains attachments
- asks for your username, password or other personal data
- wording does not have the level of refinement or sophistication expected from an authentic vendor message (e.g., misspelled words, poor grammar)
- vendor contact may have been sent direct to an employee’s University email or phone number in an attempt to circumvent established controls
- contact is asking for immediate action on their request (may try to garner sympathy, indicate a crisis such as a payment overdue and service subject to cancellation)
- Requests are coming from generic or “free” email addresses such as mail.com, Hotmail, yahoo or gmail
What is Your Response to Phishing Schemes?

- In particular don’t switch payment methods without several sources of confirmation
- Always follow the established Vendor Verification procedures
- Established procedures will include:
  - contacting the sender by an alternate method to validate the instruction
  - Employing dual control prior to making payment changes or processing payments
  - Validating that presented invoices are legitimate
Recognizing Fake URLs

► Understanding a few simple rules can help you spot a fraudster:

1. By simply hovering over the link with your mouse the URL will appear in your browser or status bar (the bar that is usually at the bottom of your screen) and you can see what the name of the site is before you actually click on it.

2. Legitimate companies use a domain name as part of their name rather than the “@” sign

3. Some URLs look very much like the name of a well-known company but some letters may be transposed or left out; instead of Microsoft.com it might read Mircosoft.com. Look carefully because these slight differences can be easy to miss!
What Makes Uncovering Fraud in Higher Ed Challenging?

- Decentralized Environment
  - Responsibility for risk management divested across campus
- Culture that frowns upon control/oversight
- Lack of formal training with Department and/or College heads of their fiduciary responsibilities for fraud
- Overall employee trust factor
Strategies for Preventing Fraud

- Never allow one person to control a process from beginning to end - identify and implement separation of duties for every process
- Strive for a strong “tone at the top” throughout the University
- Don’t ignore red flags – “know your enemy”
- Continually identify and take stock of vulnerabilities
- Data Monitoring
- Auditing of financial statements and reports
- Employee fraud awareness training
- Keeping up with fraud trends – what are other Universities getting hit with?
Strategies for Preventing Fraud cont’d

► Fraud Reporting hotlines
► Set sustainable corrective action plans that are both realistic and attainable
► Be consistent in handling of problems when they arise – the “grapevine” is a very powerful tool for preventing fraud across campus
► Most importantly…….

IF YOU SEE SOMETHING, SAY SOMETHING!
Tests
Accounts Payable (AP) Tests

- Duplicate Payments
- Split Invoices
- Payment date before invoice date
- Employee as a vendor
- Payments on non-business days or outside of normal business hours
- Round dollar or negative invoice amounts
- Payments to inactive or non-existent vendors
- Average number of days between invoice date and payment date
Accounts Payable (AP) Tests cont’d

- Above average number or dollar amount of payments to a vendor
- Invoices without valid POs or vouchers
- Missing or out-of-sequence check numbers
- Payments that exceed invoice, PO, or voucher amounts
- Vendors with a Mail Drop as a Physical Address
- “Smile but Dial” – Look at Phone Numbers on Vendor Accounts
Expense Tests

- Duplicate expense reimbursements
- Split expense reimbursements
- Close review of any manual checks issued
- Expense reimbursements after employee termination
- Expense reimbursements to non-existent (ghost) employees
- Top employees by spend and/or number of expense reimbursements
- Expense reimbursements for unallowable vendor, good/service, amount
- Expense reimbursements for travel during holidays, University breaks
Procurement Tests

- Items procured without authorization or above approved $ thresholds
- High volume of procurements from same vendor
- Procurements from vendors without proper evidence of bid/quote
- Prices greater than market average/standard
P-Card Tests

- > P-card balance exceeds authorized limit
- > Purchases made on weekends and/or holidays
- > Purchases with unauthorized vendors/merchant category codes (MCC)
- > Split P-card transactions
- > Duplicate P-card transactions
- > Purchases above single-transaction limits
- > Terminated or unauthorized employees with active P-cards
- > Employees with multiple P-cards
- > Unapproved/unallocated P-card transactions
- > Dormant P-cards
Vendor-Related Tests

- Duplicate vendor records
- Invalid Employer Identification Number (EIN) or SSN (for individuals who are sole proprietors/consultants)
- Incomplete vendor record – missing address, phone number, EIN/SSN, etc.
- Vendor records that match employee records
Internal Controls
Why Does the University Need Internal Controls?
Principles of Internal Control

https://youtu.be/9OBRg5TK9iM
Preventative vs Detective Controls
Preventative Controls

- Vendor research
- Segregation of Duties
- Detailed review and approval processes
- Central purchasing offices (e.g., Departments do not have independent purchasing authority)
- Job rotation/mandatory vacation
- Effective human resource practices – hiring & employee support practices
- Established approval processes for purchases exceeding certain thresholds
Preventative Controls cont’d

- Multiple review required for any new vendor
- Determination of whether or not any conflicts of interest exist
- Constant review of vendor database
- Vendor Code of Conduct
Detective Controls

- Internal Audit
- Budget to Actual Analysis
- Analyzing purchasing trends
- P-Card spend analysis
- Effective management review
- Engaged leadership team
Fraud Landscape -
We Are Not Alone
Coastal Carolina University scammed out of more than $1M

By: Jo Brown

Coastal Carolina University is working with multiple law enforcement agencies to investigate a scheme that resulted in a $1 million loss.

According to a news release from CCHS, the money was lost as a result of a phishing scam. The announcement came after the university found out that an email had been sent to an employee with a malicious attachment.

We Are Not Alone

Southern Oregon University loses $1.9m in email scheme

Officials wired money to a bank account

By: Sharyn Wasserstrom

Southern Oregon University has announced that it lost $1.9 million in an email phishing scheme.

The Associated Press reports that the university is now working with law enforcement agencies to investigate the incident.

The Daily Tribune reports that the university officials discovered the loss on April 10. At the time, a university spokesperson said that the university had received an email from a vendor with a suspicious attachment.

The university informed the vendor that the attachment contained malware and asked the vendor to remove it. The vendor complied, but the university then began receiving fraudulent payments.

The university lost $1.9 million in a single day, and the fraud continued for several days. The university is now working with law enforcement agencies to investigate the incident.

We Are Not Alone
Former MU employee admits to stealing from university

By: Madison Fleck | Matt Rapsdale
Posted: Nov 19, 2018 02:12 PM CST
Updated: Nov 19, 2018 03:12 PM CST

COLUMBIA, Mo. - A former University of Missouri employee admitted to stealing at least $2,500 from accounts she managed through the Wellness Center and the Student Recreation Center, according to court documents filed

Former College Employee Pleads Guilty To Stealing $173K From College; Faces Up To 20 Years In Prison

By:  November 16, 2018  |  Alex Hennes

Michael Kincie, the former director of Auxiliary Services at Connecticut College, pleaded guilty Wednesday to one count of wire fraud relating to an embezzlement scheme through which federal prosecutors say he stole vast sums of money from the College.

During his tenure as auxiliary services director, Mr. Kincie managed to run a variety of illegal operations that defrauded the College of $775,000. These activities included: recovering funds from the college through fraudulent billing schemes, diverting checks to the college to a bank account he controlled, diverting money from the Career Card program to bank accounts he controlled, and misappropriating a college laptop, according to the office of the U.S. Attorney for the District of Connecticut.

In his 12 years at the College, Mr. Kincie appeared to be a rising star in the dining services and was profiled

Washington University Embezzler Basia Skudrzyk Pleads Guilty in $300,000 Fraud

By: Debra Murphy on Tue, Dec 6, 2016 at 2:00 pm

An ex-business director estimated $300,000 from Washington University, authorities say.

A former Washington University employee who paid trips across the world, jewelry and even her divorce lawyer with embezzled money has pleaded guilty to three counts of federal mail fraud.

Barbara "Basia" Skudrzyk, 36, ran a variety of scams from May 2010 through
We Are Not Alone cont’d

Former U of M ticket director charged with fraud
Thirty-seven-year-old Brent Holck, of Maple Grove, is accused of siphoning money from football, hockey and basketball ticket orders from April 2012 to January 2017. Holck is charged with wire fraud in federal court.

We know that doesn’t make it right. Why a former PSU employee faces felony charges
BRETT PALICOTTO
SEPTEMBER 11, 2018 12:49 PM, UPDATED SEPTEMBER 17, 2018 12:40 PM

A former Penn State employee bought an Apple MacBook Pro with her university-issued purchasing card, but then sold it and kept the money, according to police.

OU audit shows improper use of state vehicle led to firing
OU: Associated Press / July 26, 2018

Jabir Shumate stands on the Senate floor at the Oklahoma state capitol in 2014. Shumate, the former vice president of University Community at the University of Oklahoma, is a former state senator from Tulsa. (Al Filipfoto/Picasa)

OU audit shows improper use of state vehicle led to firing

OKLAHOMA CITY (AP) — The University of Oklahoma’s former chief diversity officer illegally used a university vehicle hundreds of times to commute to and from work and make personal family trips, according to an internal OU audit released on Thursday.

The audit was requested after allegations surfaced about improper use of an OU vehicle by Vice President of University Community Jabir Shumate. The former state senator was hired three years ago amid campus unrest after videos surfaced showing fraternity members singing racist chants.

The audit includes GPS data that shows Shumate’s university-owned 2016 Chevrolet Tahoe parked overnight at his residence hundreds of times. It also shows Shumate took the vehicle to Tulsa over the Thanksgiving and Christmas holidays, including stops at his mother’s home.

Shumate resigned from the university this week. On Wednesday, he held a news conference where he said he was forced to step down based on false allegations that amounted to a “high-tech lynching.”

In a statement Thursday, Shumate said he is unequivocally of the information contained in the audit and says its release is part of an attempt by OU officials to “assassinate my character.”

“The university was well aware of my vehicle usage and therefore sanctioned it,” Shumate said.
Other Types of Fraud in Higher Ed

- Deans/chairs create phony positions and hire friends or relatives into them.
- Faculty inventions developed through university-sponsored research funds are marketed or sold through faculty’s private companies.
- Employees engage in consulting work on the side but use University labs and facilities or assign students to perform the consulting work.
- Department heads use Department funds to purchase goods and services for their personal use.
- Athletics - Athlete eligibility, academic fraud, scholarship awards, “pay for play”.
Consequences of Fraud

- Reputational Damage
- Monetary Loss
- Decreased Enrollment
- Risk of Reduced Grant Funding
- Civil or Criminal Court Proceedings
- Disruption of Business
  - Resources diverted to crisis
- Damaged Workplace Morale
  - Co-workers feel betrayed
Final Thoughts

- Expect ethical behavior from yourself as well as others
- Never sign or approve something you don’t understand
- Limit approval authority and don’t let anyone sign your name or use your password to give approval to a document or transaction. Signature stamps, while convenient, are typically not a good idea
- If something doesn’t make sense to you keep asking questions until it does. There really never is a “stupid question” when it comes to making sure we are all doing the right thing
- Be familiar with the University, State, or federal policies or regulations that govern your work. Be willing to call and ask questions – again – there really never is a “stupid question”
- Don’t be afraid to talk about fraud – Discuss what fraud looks like and what to do if you have suspicions
Questions?