



Overview of Fraud Prevention and Detection - Part 2

Deeper Dive using Case Studies

Niki Countryman CPA, CIA, CMA, CFE
Senior Internal Auditor
System Office of Audit and Consulting Services



May is International Internal Audit Awareness Month



What Is Internal Auditing?

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations.

At its simplest, internal auditing involves identifying the risks that could keep an organization from achieving its goals, making sure the organization's leaders know about these risks, and proactively recommending improvements to help reduce the risks.

Learning Objectives

- Fraud Overview
- Fraud Scenarios
 - Discussion
 - Red Flags
 - Prevention and Detection
- Let's Review
 - Prevention and Detection Controls
 - What can you do?
- Resources

Occupational Fraud



- Theft Embezzlement
- Financial Statement Fraud
- Asset Misappropriation



Fraud Scenario #1

Collegiate Athletics



UNIVERSITY
of ALASKA
Many Traditions One Alaska

When Major League Money Meets Little League Controls



By Herbert W. Snyder,
Ph.D., CFE; David O'Bryan,
Ph.D., CFE, CPA CMA

- Six employees conspired to improperly sell or use approximately 20,000 KU athletic tickets from 2005 through 2010.
- The sales ranged from 1 million at face value to 3 million at market value.
- Investigators were unable to determine the number improperly sold because the employees disguised the tickets as complimentary or inventory tickets.
- The investigation did not examine years prior to 2005 because KU did not retain those records.
- The director of the ticket office was making as much as \$75,000 to \$100,000 a year in additional income.
- This fraud was not discovered until a report surfaced in March of 2010 that tickets were being scalped from within the Athletic department.



Misappropriation of Assets

Review the following receipts for 10 minutes.

Discussion

1. What are some red flags?
2. How could this fraud have been discovered earlier?
3. How could this fraud have been prevented?

Fraud Prevention: Misappropriation of Assets

Red flags:

- Lax control over ticket inventory
- Culture – “Atmosphere similar to worker in a candy store”
- No set classification for tickets categories

How could this fraud have been discovered earlier?

- Restrict Access to ticket inventory
- Reconcile ticket sales

How could this fraud have been prevented?

- Segregation of Duties
 - Access to Tickets and Cash
 - Recording sales in financial software
 - Authorizing sales of tickets
- Tone at the Top

Fraud in Collegiate Athletics

When Major League Money Meets
Little League Controls



By Herbert W. Snyder, Ph.D., CFE;
David O'Bryan, Ph.D., CFE, CPA CMA

Outcome:

- Reputational damage
- Decreased employee moral
- Loss of 1 million in ticket revenue
- Civil charges against employees for:
 - Destruction of ticket records
 - Opening a “fake bank” account
 - Financial statement fraud
- HR issues
 - Decreased employee moral
 - Increased employee turnover - both director and associative director were fired



Fraud Methods

Get a employer to write a fraudster a check!

- Accounts Payable
 - Altered Receipt
 - Fraudulent Vender
 - Inflated Invoice
 - Fraudulent Employee Reimbursements
- HR – Payroll
 - Ghost employee
 - Switch direct deposit information

Fraud Scenarios #2

Employee Expense Reimbursements





Asset Misappropriation: Fraudulent Disbursements

Expense reimbursement schemes:

The most common disbursement frauds are:

- Mischaracterized expense reimbursements
- Fictitious expense reimbursements
- Overstated expense reimbursements
 - Altered receipts
 - Over purchasing
- Multiple reimbursements

Sample Documentation Red Flag



Hey Drew,


✓ **Your order is confirmed!**

Thanks for shopping! Your order [Osprey Quasar Laptop Backpack](#) and [2 more items](#) hasn't shipped yet, but we'll send you an email when it does.

Order: [#108-2982620-6230637](#)

[View or Manage Order](#)

Sub-total	\$72.92
+ Tax	...
Total	\$72.92



[Osprey Quasar Laptop Backpack](#)

Sold by: Osprey

\$72.92

Sample Documentation Red Flag



Final Details for Order #114-3301594-8659448

[Print this page for your records.](#)

Order Placed: January 23, 2020
Amazon.com order number: 114-3301594-8659448
Order Total: \$36.70

Shipped on January 24, 2020

Items Ordered

1 of: Quartet Combination Magnetic Whiteboard Calendar & Corkboard, 17 x 23 inches Combo White Board & Cork Board, Black Frame (79275)
Sold by: Amazon.com Services LLC

Condition: New

Price

\$22.09

Shipping Address:

Robb Hartman
1234 Lane Ave.
Pueblo, CO 81001
United States

Shipping Speed:

One-Day Shipping

Shipped on January 23, 2020

Items Ordered

1 of: Frigidaire 807047901 Water Inlet Valve
Sold by: Amazon.com Services LLC

Condition: New

Price

\$13.23

Shipping Address:

Robb Hartman
1234 Lane Ave.
Pueblo, CO 81001
United States

Shipping Speed:

One-Day Shipping

Payment information

Payment Method:

Mastercard | Last digits: 4523

Billing address

Robb Hartman
2200 Bonforte Blvd.
Pueblo, CO 81001
United States

Item(s) Subtotal: \$35.32

Shipping & Handling: \$0.00

Total before tax: \$35.32

Estimated tax to be collected: \$1.38

Grand Total: \$36.70

Credit Card transactions

Visa ending in 4420: January 24, 2020: \$36.70

To view the status of your order, return to [Order Summary](#).



UNIVERSITY
of ALASKA
Many Traditions One Alaska

Fraud Prevention: Fraudulent Reimbursements

Review the following receipt for 10 minutes.

Discussion

1. What are potential Red flags?
2. How could this fraud have been discovered earlier?
3. How could this fraud have been prevented?



Hey Drew,

✓ Your order is confirmed!

Thanks for shopping! Your order [Osprey Quasar Laptop Backpack](#) and [2 more items](#) hasn't shipped yet, but we'll send you an email when it does.

Order: [#108-2982620-6230637](#)

[View or Manage Order](#)

Sub-total	\$72.92
+ Tax	-
Total	\$72.92



[Osprey Quasar Laptop Backpack](#)
Sold by: [Osprey](#)

\$72.92

Order Confirmation, not invoice

Where are the other 2 items?

If there are 3 items, why is the total, the same as the one item?



UNIVERSITY
of ALASKA
Many Traditions One Alaska



Final Details for Order #114-3301594-8659448

[Print this page for your records.](#)

Order Placed: January 23, 2020
Amazon.com order number: 114-3301594-8659448
Order Total: \$36.70

Shipped on January 24, 2020

Items Ordered

1 of: Quartet Combination Magnetic Whiteboard Calendar & Corkboard, 17 x 23 inches Combo White Board & Cork Board, Black Frame (79275)
Sold by: Amazon.com Services LLC

Condition: New

Price

\$22.09

Shipping Address:

Robb Hartman
1234 Lane Ave.
Pueblo, CO 81001
United States

Shipping Speed:

One-Day Shipping

Why not shipping to UA?

Shipped on January 23, 2020

Items Ordered

1 of: Frigidaire 807047901 Water Inlet Valve
Sold by: Amazon.com Services LLC

Condition: New

Price

\$13.23

Shipping Address:

Robb Hartman
1234 Lane Ave.
Pueblo, CO 81001
United States

Shipping Speed:

One-Day Shipping

Needs justification

Different payment
methods

Payment information

Payment Method:

Mastercard | Last digits: 4523

Billing address

Robb Hartman
2200 Bonforte Blvd.
Pueblo, CO 81001
United States

Credit Card transactions

Visa ending in 4420: January 24, 2020: \$36.70

Tax

Item(s) Subtotal: \$35.32

Shipping & Handling: \$0.00

Total before tax: \$35.32

Estimated tax to be collected: \$1.38

Grand Total: \$36.70

To view the status of your order, return to [Order Summary](#).



UNIVERSITY
of ALASKA
Many Traditions One Alaska

Fraud Prevention: Fraudulent Expense Reimbursements

Red flags:

- Fuzzy support / details
- Missing, altered, generic, or non-original receipts
- Does it pass the “sniff” test
- Duplicate purchases on Procard on the same approximate date, time, and amount.

What to monitor:

- Detailed expense reports should include:
 - Detailed receipts or other supporting documentation
 - Specific business purpose
 - Date, place, and amount
- Expense report is submitted months after the purchase
- Receipts are illegible – (torn, faded, smudged)
- DO NOT share your ProCard with ANYONE.

Fraud Scenario #3

Fraudulent Credit Card Purchases



UNIVERSITY
of ALASKA
Many Traditions One Alaska

Fraudulent University Credit Card Charges



- Executive director charged with grant theft for fraudulent credit card purchases of \$43,775.02.
- Officers said they were notified by Gulf Coast State College's attorney of reported misuse of college funds dating back to 2018.
- Auditors for the college found that Mazur had "undocumented charges on a college credit card," according to PCPD. Officers also said the charges were not related to college business and not supported by documentation as required by the Foundation.
- Director resigned from her position on Nov. 14, 2020.
- It is reported by police that a warrant for grand theft was sent out for Mazur, and she turned herself in on April 14, 2021.
- According to PCPD, this case remains under investigation and additional charges could be pending.

Fraud Prevention: Fraudulent Expenses

Review the following receipt for 10 minutes.

Discussion

1. What are some red flags?
2. How could this fraud have been discovered earlier?
3. How could this fraud have been prevented?

Fraud Prevention: Fraudulent Expenses

Red flags:

- Lack of supporting documentation
- Governance without accountability – Tone at the top
- Missing, altered, generic, or non-original receipts
- Business purpose for the purchases

What to monitor:

- Detailed expense reports should include:
 - Timely submission of receipts
 - Detailed receipts or other supporting documentation
 - Specific business purpose
 - Date, place, and amount
- Does it pass the “sniff” test
- Conflict of Interest – Employees able to purchase with out review.

Fraud Scenario #4

Phishing Attacks



IRS warns university students and staff of impersonation email scam

- WASHINGTON — The Internal Revenue Service today warned of an ongoing IRS-impersonation scam that appears to primarily target educational institutions, including students and staff who have ".edu" email addresses.
- The IRS' phishing@irs.gov has received complaints about the impersonation scam in recent weeks from people with email addresses ending in ".edu." The phishing emails appear to target university and college students from both public and private, profit and non-profit institutions.
- The suspect emails display the IRS logo and use various subject lines such as "Tax Refund Payment" or "Recalculation of your tax refund payment." It asks people to click a link and submit a form to claim their refund.

University of Southern Indiana



- At least 20 accounts that were broken into, which resulted in another 44,000 emails being sent out.
- The email looked like it was from the USI IT Help Desk, and said the student or faculty member had reached their email quota and asked them to click a link.
- If you clicked the link and entered your password, IT says your password has been stolen. If this happened to you, do this immediately:
 - change this password ANYWHERE ELSE YOU USE IT (banking, credit cards, Facebook, etc.). The hacker will try to use this password anywhere they can
 - never use this password again. The hacker will keep this password (and sell it to other hackers) and they will continue to try to break into any account you have in the future



University of Alaska Phishing Attacks

Dear Staff

This is to inform you that you have been awarded a performance bonus of \$450. Kindly confirm and accept the award by following the simple steps below;

1. Log in to [UAONLINE](#)
2. Navigate to the
3. Check to see if your bonus has been added to the current paystub

Note: Allow atleast one payroll period for the bonus to be added to your account if it isn't already there.

Fraud Prevention: Phishing Attack

Please discuss the phishing emails for 5 minutes.

Discussion

1. What are some Red flags?
2. What steps can employees use to prevent fraud?
3. What could be the goal of these Phishing attacks?

University of Alaska Phishing Attacks

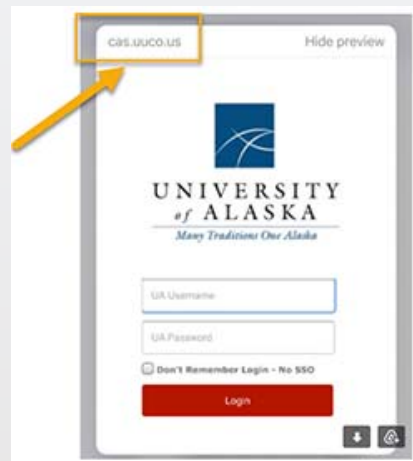
Example #2

Attention UA students and employees,

There have been a number of very convincing Phishing emails sent to alaska.edu accounts asking recipients to enter their username and password at UAOnline. The subject lines include eRefunds or Direct Deposit Information. Do not enter your username and password on the fake UAOnline login page.

If you receive a suspicious looking link, you can check it out by rolling over it with your cursor to see where the link is going. If it is not going to a location you recognize, do not click on it. In these phishing emails, the link to the fake UAOnline indicates it is going to another location (<https://cas.uuco.us>...) when you roll over it.

The link sends the user to a fake UAONLINE with a screen that looks a lot like the UA single sign-on site. Notice the cas.uuco.us in the corner, which is a tip-off that this is not our link. Plus, our SSO screen has additional information.



University of Alaska Phishing Attacks

Dear Staff

Odd phrasing

This is to inform you that you have been awarded a performance bonus of \$450. Kindly confirm and accept the award by following the simple steps below;

1. Log in to **UAONLINE**
2. Navigate to the
3. Check to see if your bonus has been added to the current paystub

Link to cas.uuco.us

Misspelling

Note: Allow atleast one payroll period for the bonus to be added to your account if it isn't already there.

Fraud Prevention: Unauthorized Access - Cyberattacks

Red flags:

- Spoof URL does not match (hover mouse over)
- Asks for UAID or Password
- Emails promising a reward, cash payment - too good to be true
- Odd wording or grammar

Fraud Prevention:

- Change password if you suspect illicit activity
- Notify IT of suspicious emails
- Do not forward, open any attachments or click on any links
- Never share your UA ID or password

Let's Review



Review Questions

What to do when you suspect fraud has occurred?

- a. Conduct your own investigation.
- b. Confront the individual with an allegation of fraud.
- c. Ignore it.
- d. Discuss it with your supervisor or make a UA anonymous hotline report at:

alaska.ethicspoint.com

Review Questions

What is the fraud factor that an organization can control?

- a. Pressure.
- b. Opportunity.
- c. Rationalization.
- d. Capability.

Review Questions

What are signs of a phishing email:

- a. Emergency requests to change account information
- b. Requests for Passwords
- c. Sentences or numbers separated by commas instead of periods
- d. All of the above

Review Questions

How is the vast majority of occupational fraud detected?

- a. Internal audit
- b. Surveillance
- c. Tips
- d. Accidental discovery

University of Alaska System Office of Audit and Consulting Services

Additional training resources and presentation slides

System Office of Audit and Consulting Services Website

<http://www.alaska.edu/audit/>

- A&CS Internal Controls
- Self-Assessment Questionnaires
- Fraud and Internal Controls Presentations

For more information, contact

Niki Countryman, CPA, CIA, CMA, CFE

Senior Internal Auditor

(907)786-7756

nrcountryman@alaska.edu or

A&CS Department email: ua-ia-dept@alaska.edu

UA Confidential Hotline

Hosted by NAVEX Global "EthicsPoint"

- EthicsPoint is used by hundreds of higher education institutions
- Third-party hosted to provide the best option for anonymity
- Available via
 - web intake alaska.ethicspoint.com
 - toll-free telephone (855-251-5719)
- Different types of issues/concerns can be reported:
 - Financial: fraud, waste, abuse
 - Ethical misconduct
 - Safety and environmental
 - Compliance
 - Human resources (i.e.: bullying)
 - Protection of minors



Presentation Resources

- 2020 ACFE Report to the Nations on Occupational Fraud & Abuse, Association of Certified Fraud Examiners.
- Auburn University, Case in Point: Lessons for the proactive manager
- The Fraud Diamond: Considering the Four Elements of Fraud. David T. Wolfe and Dana R. Hermanson. 2004



Fraud Prevention and Detection

It Starts with You!



UNIVERSITY
of ALASKA
Many Traditions One Alaska