CAN IT HAPPEN TO YOU?

THE ANSWER MIGHT SURPRISE YOU!
Welcome to the Session

- Name
- Agency
- Role
- What you would like to learn at this day of training
SESSION GOALS

01 Define Fraud, Waste & Abuse
02 Define IT Vulnerabilities
03 Define Internal Controls
04 Assign Responsibility
FRAUD, WASTE & ABUSE

**Fraud** – An intentional deception that violates a law or the public trust for personal benefit or the benefit of others.

**Waste** – Behavior involving the extravagant, careless, or needless use of government funds, property, and/or personnel.

**Abuse** – Behavior involving the use of government funds or property that a prudent person would not consider reasonable and necessary business practice given the facts and circumstances.
OBSERVATIONS FROM RESEARCH

- **Three risk areas**
  - People, money & opportunity
  - To some degree, the only thing we can limit or attempt to control is opportunity

- **Ray’s Reasoning**
  - You either have had, do now, or will hire in the future, a person willing to commit fraud if given the proper set of circumstances and opportunity to do so

- **Trust BUT Verify**
United States Attorney Ron Parsons announced that an Eagle Butte, South Dakota, woman [age 35] has been indicted by a federal grand jury for **Embezzlement and Theft** from a Tribal Organization and Larceny.

The maximum penalty upon conviction is **5 years in federal prison and/or a $250,000 fine**, 3 years of supervised release, and $100 to the Federal Crime Victims Fund. Restitution may also be ordered.

The Indictment alleges that on or about between the 27th day of February, 2015, and the 13th day of March, 2015, the accused, being an employee of an Indian tribal organization, that is, the cashier of the Cheyenne River Sioux Tribe Bingo Operations, **embezzled** and converted to her own use over $1,000 of the moneys, funds, and credits belonging to the **Bingo Operations**.
Baltimore, Maryland – A federal grand jury has indicted [the accused], age 43, of Baltimore, Maryland, on federal charges in connection with a scheme in which the accused allegedly filed fraudulent claims for Social Security benefits using **fictitious identities and the identities of actual individuals and attempted to collected over $236,000**. The indictment was returned on April 3, 2019.

The accused was employed by the Social Security Administration (SSA) as a Claims Specialist. The 14-count indictment alleges that between July 2018 and March 2019, the accused used his position at SSA to create **fictitious identities** within the SSA’s social security number database in order to file fictitious claims for benefits. The indictment alleges that the accused used both fictitious identities and the identities of actual individuals to file the fraudulent claims and stole or attempted to steal over $236,000 from SSA.
SSI Continued…

According to the indictment, the accused caused SSA to pay approximately $87,000 in fraudulent claims through direct deposit, issue approximately $46,000 in checks that were never negotiated, and authorize approximately $103,000 in claims that SSA halted before payments were issued.

If convicted, the accused faces a maximum sentence of 20 years in prison for each of nine counts of wire fraud; a maximum of 10 years in prison for Social Security fraud and for theft of government property; and a mandatory two years in prison, consecutive to any other sentence imposed, for each of three counts of aggravated identity theft. The accused was arrested on a related criminal complaint on March 20, 2019 and was released under the supervision of U.S. Pretrial Services. No court appearance has been scheduled yet on the indictment.
The indictment alleges that from around November 2001, continuing to around November 2011, the accused [age 37] willfully and knowingly did steal, purloin, and convert for her own use money belonging to the U.S. Department of Housing and Urban Development, having a value of approximately $88,000, by obtaining HUD Housing Choice Voucher Program rent subsidies for a home in which she had an ownership interest when she knew she was not entitled to the rent subsidies due to her ownership interest in the property.

The indictment further alleges that from November 2001, continuing to around November 2011, the accused willfully and knowingly did steal, purloin, and convert to her own use money of the Social Security Administration, having a value of approximately $72,000, by obtaining Supplemental Security Income while also receiving unreported assistance from the HUD Housing Choice Voucher Program.
The accused is also alleged to have made materially false statements to HUD and SSA in the HUD "Tenant Annual Renewal Personal Declaration" and the SSA "Redetermination Summary for Determining Continuing Eligibility for Supplemental Security Income Payments" forms when she did not disclose her ownership interest in the real estate for which she was receiving the rent subsidies and she did not disclose to the SSA the rent assistance she was receiving through the HUD Housing Choice Voucher Program.

If convicted of Theft of Government Funds, the accused faces a maximum penalty of 10 years in prison, a $250,000 fine, and three years of supervised release as to each count. If convicted of False Statement, Smith faces a maximum penalty of five years in prison, a $250,000 fine, and three years of supervised release as to each count.
CASE STUDY A

- You are monitoring the Weatherization program of XYZ Community Action.
- XYZ completely outsources all production of weatherized units (it has no staff that do construction work). You have noticed from your desk review that the cost per unit for XYZ is exactly twice what it is for the three neighboring CAPS. The Weatherization director tells you this is not possible.
You have the Finance Director assemble the following subcontractor summary:

- Able, Inc. $84,500 for 42 units
- Baker Company $150,726 for 71 units
- Charlie Corp. $327,441 for 23 units

Currently, all invoices come into the finance office and are paid directly from there. Do you have any concerns? What are your next steps? Any controls you might suggest going forward?
You have been asked to monitor ABC CAP. In the review of payroll transactions, you notice that there are two employees who make more than the Executive Director.

In the current system, payroll is prepared by the accounting clerk. She also is a “people person” so she is the defacto Human Resource Department – conducting interviews and hiring new employees.

Does this cause you any concern? What additional records might you want to review? What enhancements to internal controls would you recommend?
CASE STUDY C

- You are in River City to do the monitoring visit for the CAP. You have interviewed the program staff and are impressed with the knowledge and dedication of the program people.

- Next, you turn your attention to the fiscal office. When you arrive, 2 of the 3 fiscal staff are on vacation. About one-half of the items you asked to review are in a pile waiting for you in a small conference room.
You try tracing a transaction from January through the general ledger and get confused because it is in, out, in twice, backed out three times and then posted backwards. When you ask for clarification, you are told only the finance director knows how to use that stupid ‘generous leader’ program. You finally call the Board Treasurer for help and he says that the Board has not looked at that month yet (it’s October now).

Do you have any concerns? What ‘red flags’ are you seeing? Do you have any suggestions for improvements? If so, what are they?
Let’s look at a QCI scenario

- WAP Manager at a sub-grantee
- QCI certified
- Performs QCI inspections for neighboring sub-grantee
- Discovered through monitoring paid to perform QCI as contractor while “on the clock” being paid as WAP Manager – through same federal grant

What do you do?
“Obviously, people lie when they’re trying to hide something. I did it too.”

Statement by a fraudster | personal interview
**White Collar Criminal Characteristics**

- impeccable reputation
- abuse of professional position
- above-average level of education and creativity
- criminal energy is not discernible
- can come from any area of expertise, independent of sector
- has been working for the company for more than five years
“You can write the best manuals and draw up the best work processes – but if something is urgent, and in emergencies, things never run to plan.”

Statement by a fraudster | personal interview
FRAUDSTER CHARACTERISTICS

Radiates Trust

Even after talking to a dozen different white-collar criminals, I was still impressed at how unbelievably courteous and charming they are. It is these traits which enable fraudsters to win the trust and empathy of those around them with playful ease. To a certain extent, this character trait prevents those around them from objective assessments.

This dangerous ability creates the perfect breeding ground for fraud. Controls, for example, are neglected. As a head fraud investigator, I often hear people say, “I thought this employee was a person of complete integrity. Of all people, he was the one I would have believed least likely of committing such an offence.”
White-collar criminals approaches

- Pin-striped predator
- Hedonistic narcissist
- Gullible victim

The white-collar criminals sees himself as the victim of unfortunate circumstances. Fraudsters of this type tell me they were under enormous pressure. They explain their fraudulent behavior as their attempt to resolve an insoluble problem. Under normal circumstances, this profile of a fraudster is an exemplary employee who follows rules to the letter and would never hurt anybody. As a result, those around him are surprised and even shocked at his fraudulent behavior.
The **pin-striped predator** consciously seeks and patiently awaits opportunities to commit fraud. Such a person is remarkably disciplined and focused and translates his visions into action. His belligerent attitude makes him an opponent who needs to be taken seriously. With playful ease, he manipulates his superiors, public accountants and any regulatory bodies who have little experience in fraud. He is extremely skilled in organizing complex techniques for evading discovery. To create confusion and uncertainty in an impending investigation, he creates false leads in advance to throw others off the scent.
The **hedonistic narcissist** has an exaggerated opinion of himself, is arrogant, and is not open to criticism. He commits fraud because he is convinced, he is so uniquely clever that he’ll never get caught. Stuck in a groove, this profile of a fraudster loses all grip on reality regarding money. His sense of entitlement is obsessive. However, financial considerations are not his sole motive. He also enjoys the cat-and-mouse game, demonstrating his superiority and getting an adrenalin rush. For such a person, the chase to win admiration is exciting – and never-ending.
The **gullible victim** regards himself as a social creature. In the eyes of the fraudster, he is being exploited by profiteers. Offenders of this type do not actively search for opportunities to commit fraud. But to maintain a relationship, or to revenge themselves for a disappointment, they are willing to commit serious economic crimes. Such persons will engage in fraudulent behavior for a higher purpose, or to overcome separation anxieties.
GENERAL FRAUD FACTS

90% of Fraudsters are first-time offenders with clean records.

40 – 60% of businesses never recover any fraud related losses.

Statistics show that the average occupational case of fraud is active for 18 months before it’s detected.
Many Leaders believe they’d feel it in their gut if something were amiss.

Many nonprofits believe they’re immune to fraud because they have strong core values.

One key best practice… never build a system of internal controls based on trust.
Possible fraudulent act triggers of a White-Collar Criminal

- Personal debt
- Medical bills
- A spouse losing a job
- An ailing parent moving in
- Drug or alcohol use
- Gambling
- An inability to control spending
These six red flags was first tracked in 2008. The ACFE found that approximately 79% of perpetrators exhibited at least one of these six during their employment.

**Possible fraudulent act triggers of a White-Collar Criminal:**

- Personal debt
- Medical bills
- A spouse losing a job
- An ailing parent moving in
- Drug or alcohol use
- Gambling
- An inability to control spending

**Red Flags of a White-Collar Criminal:**

- Living beyond means
- Financial difficulties
- Unusually close association with a vendor or customer
- Wheeler-dealer attitude
- Control issues, unwilling to share duties
- Divorce/family issues
CHARACTERISTICS OF FRAUDSTERS

- 42% staff-level employees
- 36% mid-level managers
- 55% worked alone in committing their scheme
- 52% were between the ages of 31 and 45.
- Two-thirds were male
- 47% had worked for the victim organization for less than six years
- 72% had at least some university education
- 45% worked in the accounting, primary operations, or sales at the victim organization
- 87% were first-time offenders with no criminal history of fraudulent behavior
- 44% were known to be living beyond their means
Internal control is a process for assuring achievement of an organization's objectives in

- operational effectiveness and efficiency,
- reliable financial reporting, and
- compliance with laws, regulations and policies.

A broad concept, internal control involves everything that controls risks to an organization.
Internal controls are the mechanisms, rules and procedures implemented by an agency to ensure the integrity of financial and accounting information, promote accountability and prevent fraud.
Control Environment is the agency's attitude toward internal controls necessary for effective internal control, because even the best-designed systems can be thwarted if management overrides the controls that are in place.

Trust that overrides the internal control is the same as not having the internal control in place.
INTERNAL CONTROLS

- **Financial Controls** – Financial controls adopts an accounting standard and segregation of duties
- **IT Controls** – Controls related to IT operations and information security. (adding users/permissions to systems)
- **Project Controls** – Control of projects using project management, risk management, and project governance processes
- **Risk Control** – The process of identifying and controlling risk
- **Compliance Control** – Controls that are directly related to compliance
- **Safety Controls** – Safety controls in warehouse, food preparation kitchens, and weatherization work
- **Human Resources Control** – Controls related to employee performance and culture. Example – process for employee performance reviews and disciplinary policies
- **Operational Control** – Controls related to an agency’s processes such as a process of reporting results to leaders and board
- **Quality Control** – The testing of services to ensure conformance to specifications and policy
Financial controls are processes, policies and procedures that are implemented to manage finances. Controls are implemented with:

- accountabilities,
- responsibilities, and
- automation.
FINANCIAL CONTROLS

- **Financial Statements** – delivery of timely and accurate financial statements
- **Policies** – Policy for general ledger, chart of accounts, invoicing, payment processing, inventory and asset management
- **Segregation of Duties** – See next slide
- **Reconciliation** – bank statement to general ledger
- **Disbursement Policies** – validation of disbursement such as checking that each payroll payment is to a real employee
- **Audit Trail** – created and retained for events such as approvals, financial transactions and updates to financial documents
FINANCIAL CONTROLS

1. Separation of duties – is the principle that no single individual is given authority to execute two conflicting duties

Examples:

- Vendor Maintenance and Posting Invoices – Separation of creating vendors in a system from posting and paying invoices. Helps to prevent fictitious vendors/customers with fictitious invoices
- Purchase Orders and Approvals – Purchase orders typically require multiple approvals
- Payment and Bank Reconciliation – Making payments to vendors and reconciliation of bank statements
- Paychecks and Bank Reconciliation – Paying employees and back reconciliation
- Journal Entry and Approvals – Separation of entering a journal entry and approval of journal entries
- Cash and Account Receivable Reconciliation – Separating roles that manage cash deposits from customers and reconciliation of those deposits
- Hire and Set Compensation – Hiring an employee and setting their compensation. Helps to prevent people from hiring friends at an inappropriate salary
- Expenses and Expense Approvals – Separation of claiming and approving expenses.
- Asset Custody and Asset Inventory – Separation of custody of assets and record keeping related to those assets
- System Access Permissions – Adding and editing system access permissions is viewed as a root authority that is separated from all financial management activities
QUESTIONS FOR THE GROUP

- Where do you think your agency is most vulnerable?
- Do you have internal controls in place at your agency?
- If yes, are they being followed?
- If yes, how do you know?
- How are you testing your internal controls?
LESSONS LEARNED FROM LIVING THROUGH IT
LESSONS LEARNED FROM LIVING THROUGH IT

- What is the cost?
  - Staff hours
  - Stress & Anxiety
  - Financial
  - Reputational Damage
LESSONS LEARNED FROM LIVING THROUGH IT

- **Staff Hours**
  - Controller
  - Weatherization Program Manager
  - Executive Director
  - Other business office staff
  - Special meeting for 25 staff members – communication plan
LESSONS LEARNED FROM LIVING THROUGH IT

- **Stress & Anxiety**
  - Team cohesion
  - Donor relations, public perception
  - Fear of losing program
  - Perpetrator continued to interact with former co-workers who were unaware of the investigation
  - Interviews with US Federal Investigators
  - Wondering if more than one person was involved
  - Not knowing the extent of the crime
LESSONS LEARNED FROM LIVING THROUGH IT

- **Financial**
  - Reimbursement of loss from fraud to funder
  - Attorney fees
  - Contracting with a Crisis Management Team
  - Dropped from Crime Insurance, difficulty securing new policy
  - Cost of new Crime Insurance increased exponentially
  - Facility improvements no longer possible due to cost related to investigation
  - Attorney fees associated with Attorney-Client Privilege
    - Attorney present for closed session Board meetings
ROLES & RESPONSIBILITIES AT AGENCY LEVEL
What do you think the role of the Financial Manager/Director is in financial management?

- Establish policies and safeguards in accordance to 2 CFR 200 & Generally Accepted Accounting Principals
- Develop Internal Controls
- Test Internal Controls
- Never be or accept a single signature payment system
- Ensure all funds spent appropriately within program guidelines
- Ensure all federal & state reporting is correct & timely
Role list continued...

- Open and complete general ledgers that are easy to follow
- Test Internal Controls
- Establish and enforce procurement standards and practices
- Be aware of how “fraudsters” operate
- Take to heart any tips received
- Never be so removed from approval and payment processes that you do not see what is processed and paid
- Tracking proper claiming and payment of staff time and salaries
What are your thoughts on this relationship?
- Sharing of information is a NECESSITY – honest, open and often!
- FEDERAL DOLLARS!!!
- Sharing/discussion regarding the average cost per home and production
- Sharing how WAP funds are used
  - How much space rent do you pay?
  - What magazine subscriptions do you pay for?
  - How are the utility expenses shared across programs?
- How do you know LIHEAP & DOE jobs are handled correctly?
Relationship thoughts continued…

- FEDERAL DOLLARS !!!
- Needed approval from the Weatherization Manager
- Open and thorough communication is CRUCIAL!
- If something seems off, ASK QUESTIONS!
- Are changes ever made after the WAP Manager has approved the expense?
- Regular, open discussions between the WAP & Finance
- Regular, clear reporting on all expenses
IT VULNERABILITIES
5 BIGGEST RISK FOR CYBER SECURITY

- People
  - Phishing emails
  - Clicking on links
  - Downloading documents that turn out to be malware

- Passwords
  - Use strong password, and two-factor authentication (2FA)
  - Ask employees not reuse passwords from other online accounts for any of their work accounts.
  - IT policy: Make Employees change their passwords every 30 or 60 days

- Patch Management
  - Keep software updates current
  - Avoid WannaCry and Petya outbreaks - attacks spread was by exploiting a critical vulnerability in the Windows operating system known as Eternal Blue. Eternal Blue allowed the malware to spread within corporate networks without any user interaction, making these outbreaks particularly lethal.
5 BIGGEST RISK FOR CYBER SECURITY

- **Other Agencies – weak security methods**
  - Cyber security protocols of other agencies they work with. They are the weakest links.
  - Network segmentation, or dedicated servers that vendors can use so that they do not connect directly into your agency's network, can help safeguard against weak links.

- **Bring your own device – brings in trouble**
  - BYOD (Bring Your Own Device) Allowing employees to bring their own devices to work can present its own problems.
Software update supply chain attacks
Attack implants a piece of malware into legitimate software package and is released when updating software, can grow quickly and unnoticed. Attackers often target specific regions or sectors, which is what happens with the Petya/NotPetya attacks.

Safe Guards:
- Test new updates in small test environments
- Monitor activities on a system for unwanted patterns and block suspicious applications before any damage can be done
- Detect unwanted changes in the software update process by always looking at the website of software package producers. They should ensure that their web pages are always up-to-date
TOP 5 CYBER SECURITY THREATS IN 2019

- **Phishing Attacks**
  
  246,231,645 phishing attacks were detected in 2017
  
  A phishing attack is a type of social engineering attack designed to steal user logins, credit card credentials, and other types of personal, business or financial information.

  **Examples:**

  - Coming from a perceived trusted source, attack impersonates well-known and trusted websites, banking institutions or personal contacts.
    
    By entering or using credentials, clicking links or replying to phishing emails with financial details, information is sent directly to the malicious source.

  **Safe Guards:**

  - Raising employee awareness and training
TOP 5 CYBER SECURITY THREATS IN 2019

- **Ransomware**
  Around 4,000 ransomware attacks occur every day
  Ransomware has the potential to cause the permanent loss of company data, because it infects encrypted data and secure database systems and threatens to delete or corrupt files unless a ransom is paid.

Safe Guards:
- Train employees to use endpoint security solutions. In 2019, more solutions will be available.
TOP 5 CYBER SECURITY THREATS IN 2019

- Advanced Persistent Threats need Advanced Threat Protection

Advanced Persistent Threat (APT), placed on a network and quietly steals information for a significant period of time, it can collect financial information, login credentials, and more. APT enters through a file, email, network or application. It is very difficult to detect.

Traditional cyber security measures such as defense-in-depth, firewalls and anti-virus, cannot protect against an APT attack.

Safe Guards:

- Advanced Persistent Threat Protection systems and segmenting the network can help to discover unusual behavior or patterns within a network.
- FireEye’s Adaptive Defense approach can intercept possible APTs.
IoT (Internet of Things) DDoS Attacks

Networks of compromised IoT devices that can be remotely controlled and used to launch attacks on a massive scale create powerful botnets – called a Mirai attack. Botnets are controlled by Command and Control networks. The hacker runs these networks to launch distributed denial of service attacks (DDoS). IoT devices lack built-in security which makes them vulnerable.

Safe Guards:

- Using DDoS protection solutions is considered a major cyber security priority for the years to come.
TOP 5 CYBER SECURITY THREATS IN 2019

Prevention Strategies:

- Educating Employees
- Using scalable next-generation cyber security solutions
- Gaining insight into threats targeting your agency
WHAT TO DO WHEN YOU SUSPECT FRAUD
Call BCAEO’s Executive Director to discuss the situation

Options:
- Deploy the appropriate monitor to help research the issue
- Discuss talking to the Office of Inspector General
- Discuss talking to Quality Assurance Office
- Discuss talking to the Contract Unit

Notify BCAEO sooner rather than later to help assist through the process.
WHEN FRAUD WITH DISALLOWED COSTS IS UNCOVERED IN CSBG OR WAP

- Disallowed costs determined – by agency, BCAEO’s monitoring review, or Federal Office (CSBG/DOE)
  - BCAEO issues a monitoring report requesting funds to be returned to MDHHS using non-federal and non-state funds
  - Upon receipt of funds
    - BCAEO issues a management decision letter resolving the finding with disallowed costs to the agency
    - BCAEO returns funds to the federal agency
WHEN FRAUD WITH DISALLOWED COSTS IS UNCOVERED IN CSBG OR WAP

Depending on the severity of the finding and/or amount of deficiencies identified

- CSBG or DOE will issue MDHHS/BCAEO a report with findings and corrective action
  - MDHHS/BCAEO will review the report
  - MDHHS/BCAEO will pass through any agency’s findings including disallowed costs to the agency as necessary
  - MDHHS/BCAEO will develop and implement statewide corrective action (training, policy update…)
  - MDHHS/BCAEO will submit a response to the federal report on the corrective action taken by the agency and MDHHS/BCAEO

Examples:

Agency Responses

- Firing Staff
- Staff members charged for fraud
- Staff suspended and debarred
- Return of funds
- Programs terminated
- Agency De-designated
- Improved Internal Controls
- Policy Updates
- Staff Training
- Program Management Updated
Steps:

1. State conducts monitoring review

2. State determines if CAA fails to comply with the terms of an agreement, or the State Plan, to provide services or to meet appropriate standards, goals, and other requirements established by the State (including performance objectives).

3. State informs the entity of the deficiency to be corrected.
4. State requires the CAA to correct the deficiency

5. State determines whether training and technical assistance is appropriate

6. State offers training and technical assistance, if appropriate, to help correct the deficiency

7. State either (A) prepares and submits to the Secretary a report describing the training and technical assistance offered; or (B) if the State determines that such training and technical assistance are not appropriate, prepares and submits to the Secretary a report stating the reasons for the determination.
8. At the discretion of the State, the State allows the CAA to develop and implement, within 60 days after being informed of the deficiency, a quality improvement plan to correct such deficiency within a reasonable period of time, as determined by the State, and not later than 30 days after receiving from a CAA a proposed quality improvement plan, either approve such a proposed plan or specify the reasons why the proposed plan cannot be approved.

9. State provides adequate notice and opportunity for a hearing

10. State initiates proceedings to terminate the designation of or reduce the funding under this subtitle of the CAA unless the CAA corrects the deficiency.
Questions?
Comments?
Any pointers or thoughts from our discussions?
Thank you for being here!