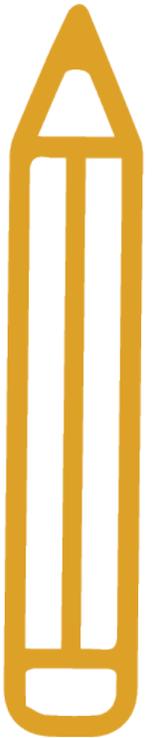
 LUNCH & 
LEARN



Questions

- Use Panel Options “Q&A”

Learning Objectives

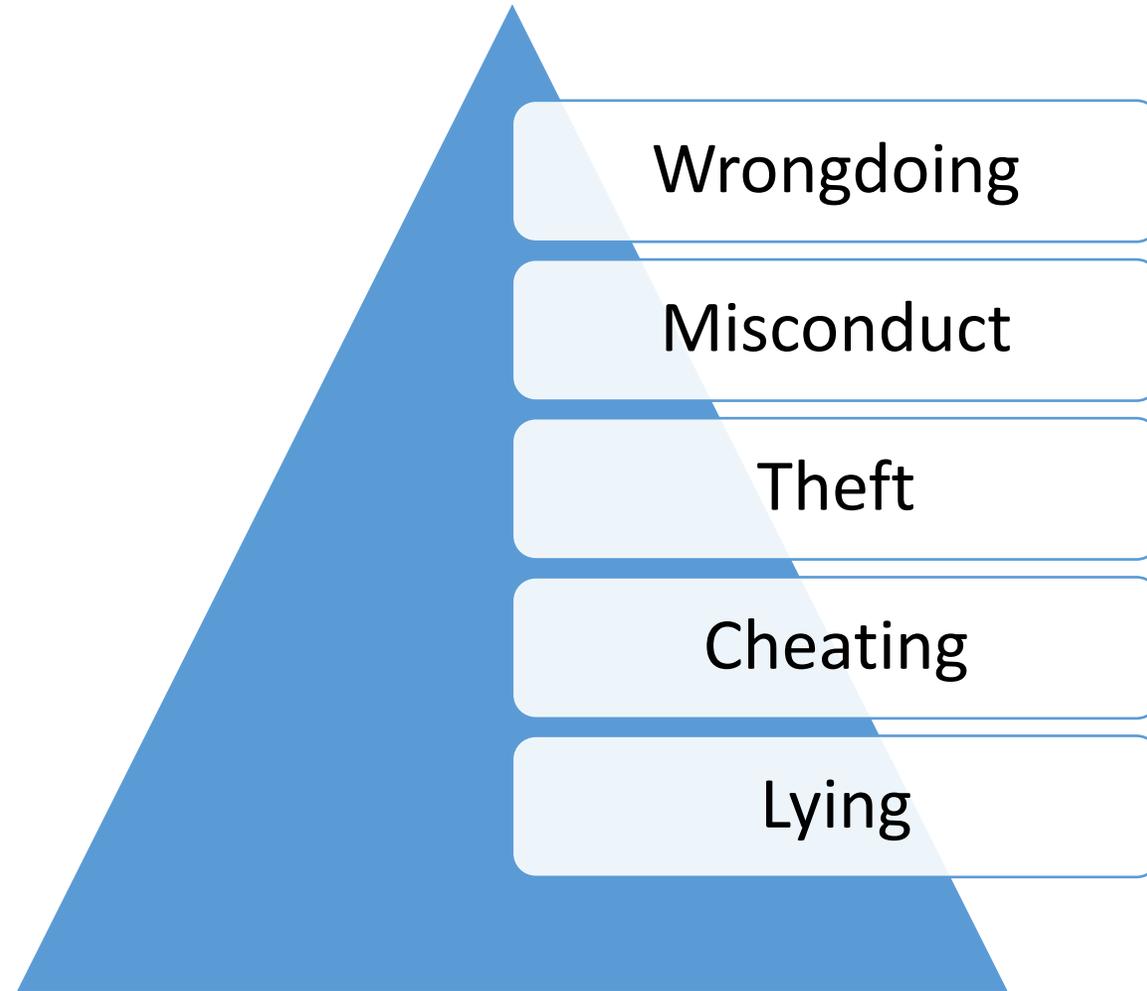
- Define what fraud is
- Provide fraud statistics – who, what, when
- Provide information on how to reduce fraud risk
- Provide information on how to report possible fraud

International Fraud Awareness Week

- November 12-18, 2023
- Organizations worldwide lose an estimated 5 percent of their annual revenues to fraud, according to [*Occupational Fraud 2022: A Report to the Nations \(ACFE\)*](#).
- Fraud takes many shapes and forms, among them corporate fraud, consumer fraud, tax fraud, identity theft and many others.



What do we mean by fraud?

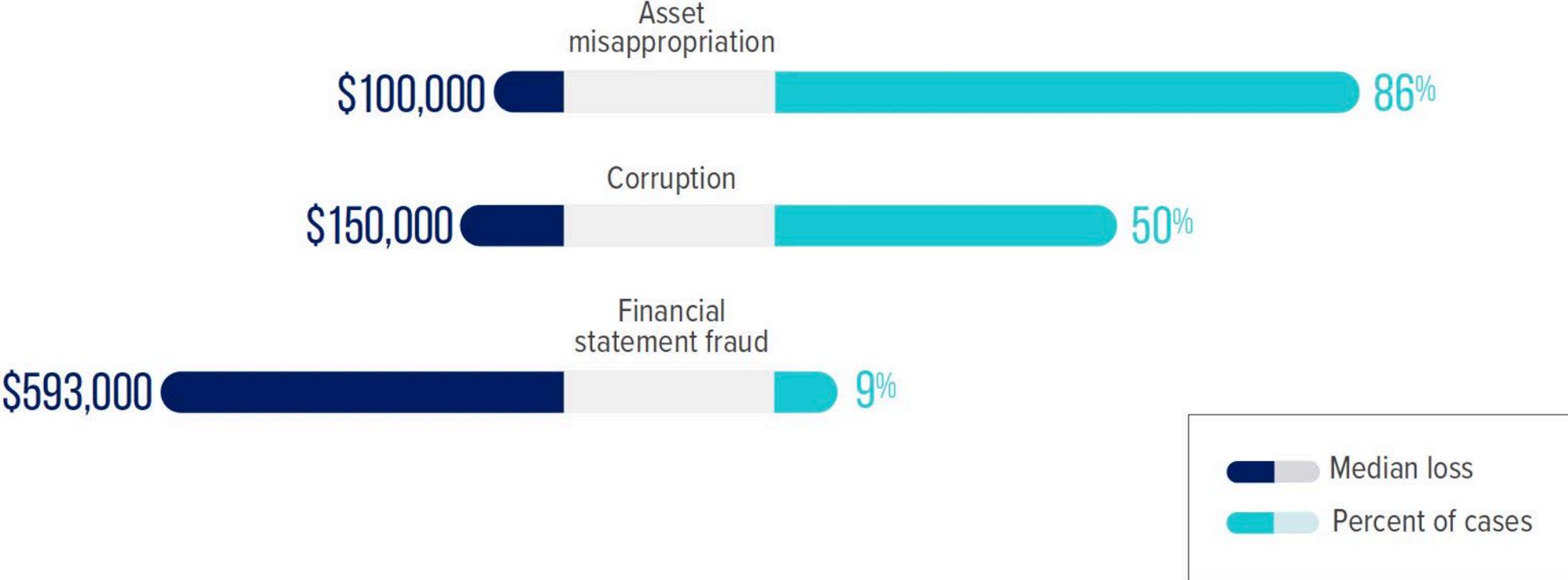


Fraud defined...

"Any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain." *

*Source: The Institute of Internal Auditors (IIA), The American Institute of Certified Public Accountants (AICPA), & Association of Certified Fraud Examiners (ACFE), *Managing the Business Risk of Fraud: A Practical Guide* (pp. 5).

HOW IS OCCUPATIONAL FRAUD COMMITTED?



WHAT IS OCCUPATIONAL FRAUD?

Asset Misappropriation Examples:

- Theft of cash, services, inventory, time or intellectual property; falsified expense reports and purchase order schemes, in which payments are made to false vendors

Corruption Examples:

- Conflicts of interest, bribery, improper gratuities and economic extortion

Financial Statement Fraud Examples:

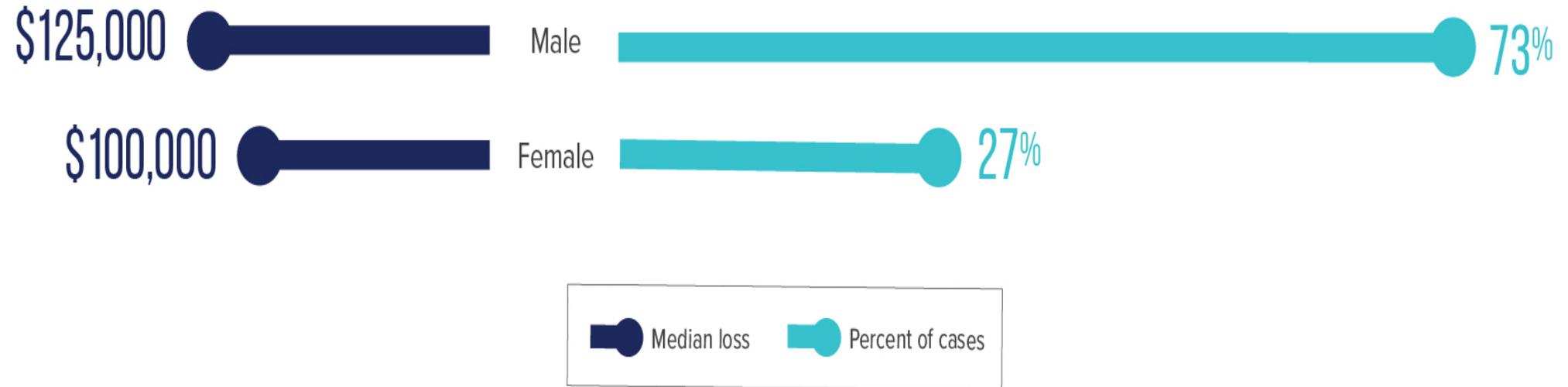
- The deliberate over/under statement of financial statement balances in many cases to make a company appear to be in better financial position
- Falsifying balance sheets or income statements



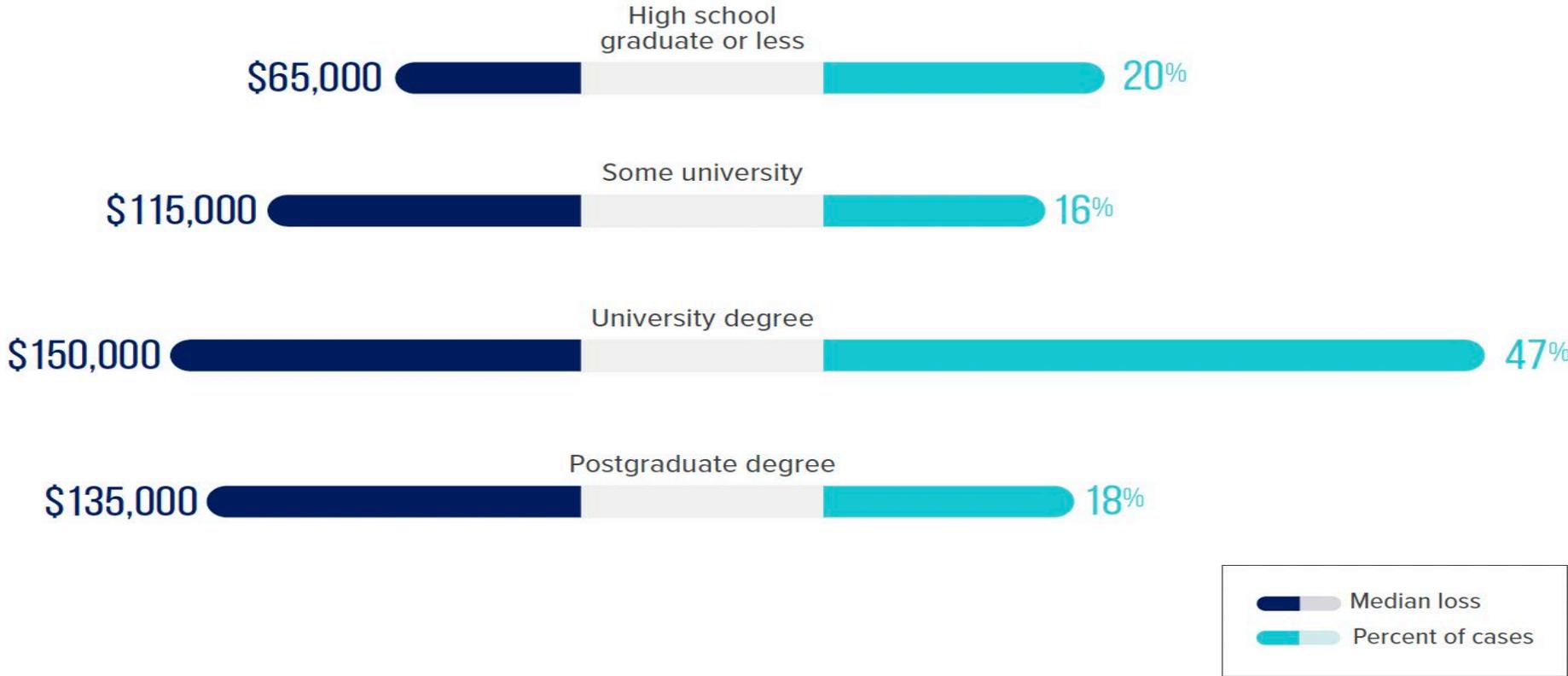
What does a “TYPICAL” Fraudster look like?



HOW DOES THE PERPETRATOR'S GENDER RELATE TO OCCUPATIONAL FRAUD?



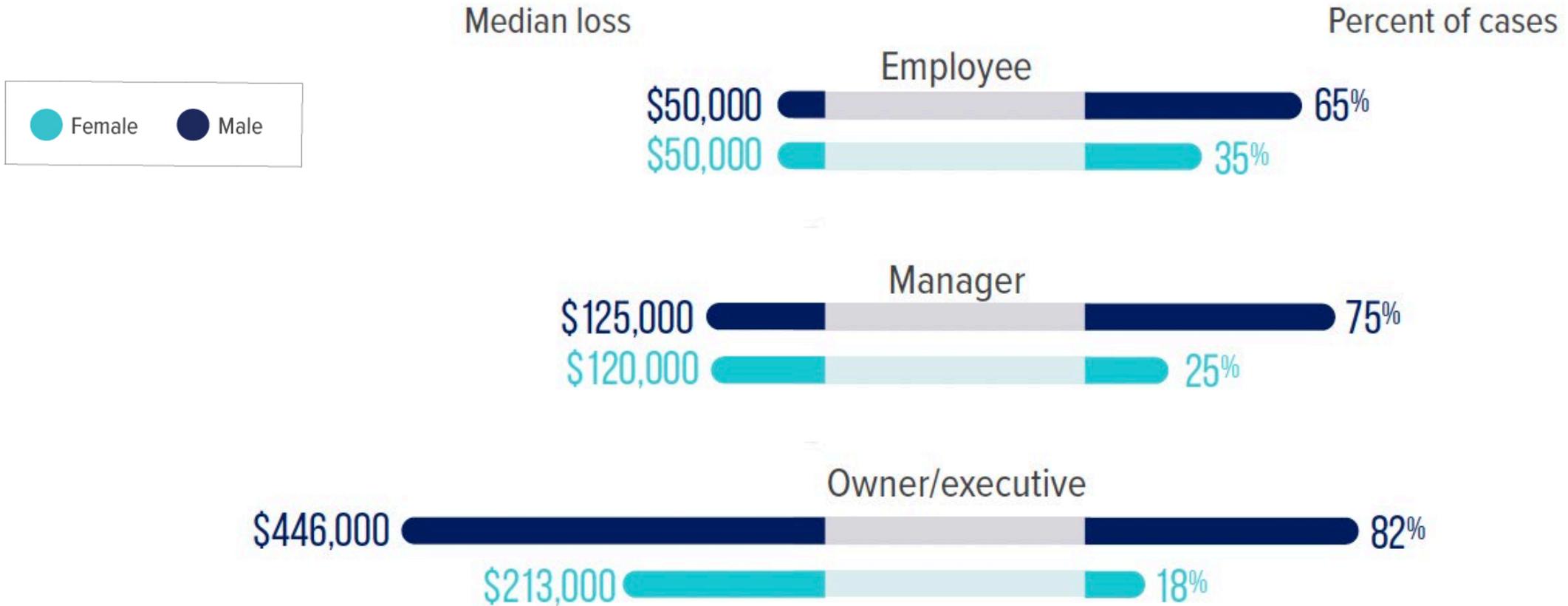
HOW DOES THE PERPETRATOR'S EDUCATION LEVEL RELATE TO OCCUPATIONAL FRAUD?



HOW DOES THE PERPETRATOR'S AGE RELATE TO OCCUPATIONAL FRAUD?



HOW DO GENDER DISTRIBUTION AND MEDIAN LOSS VARY BASED ON THE PERPETRATOR'S LEVEL OF AUTHORITY?



Fraud in Higher Education...

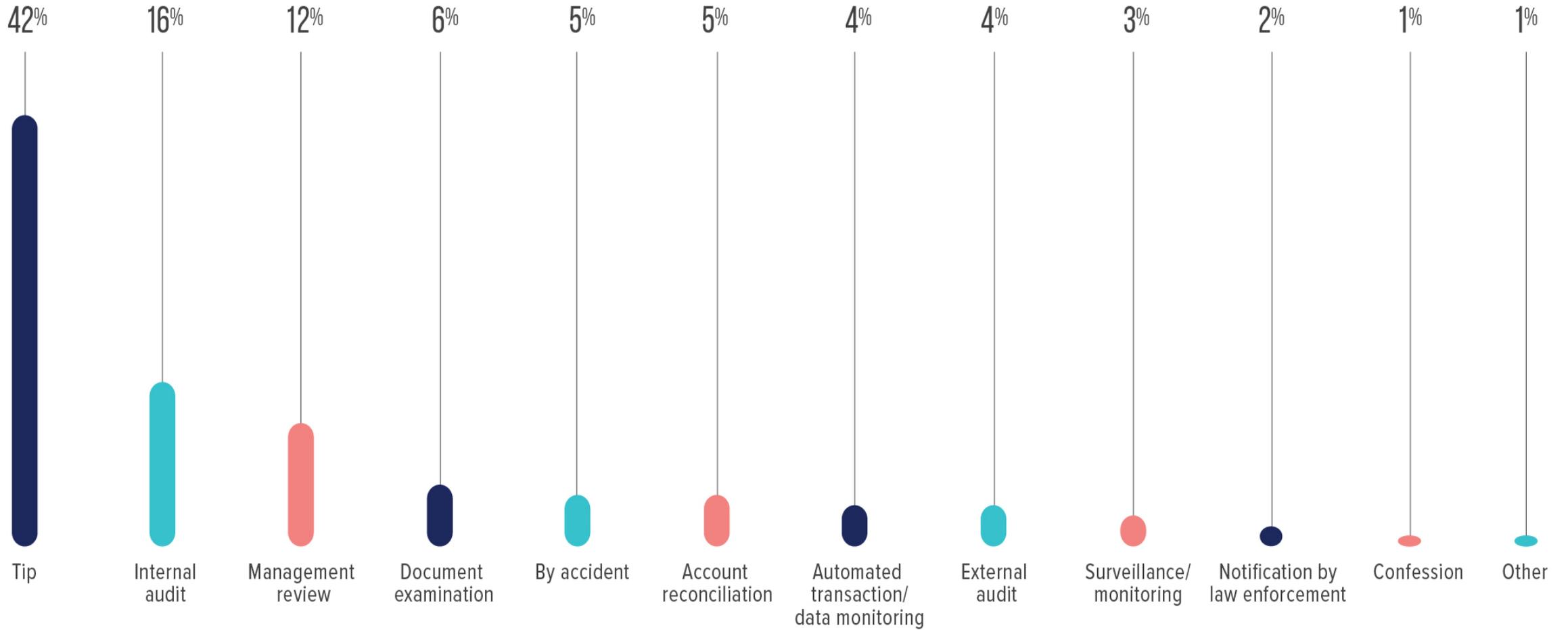
BREAKING

HEADLINES

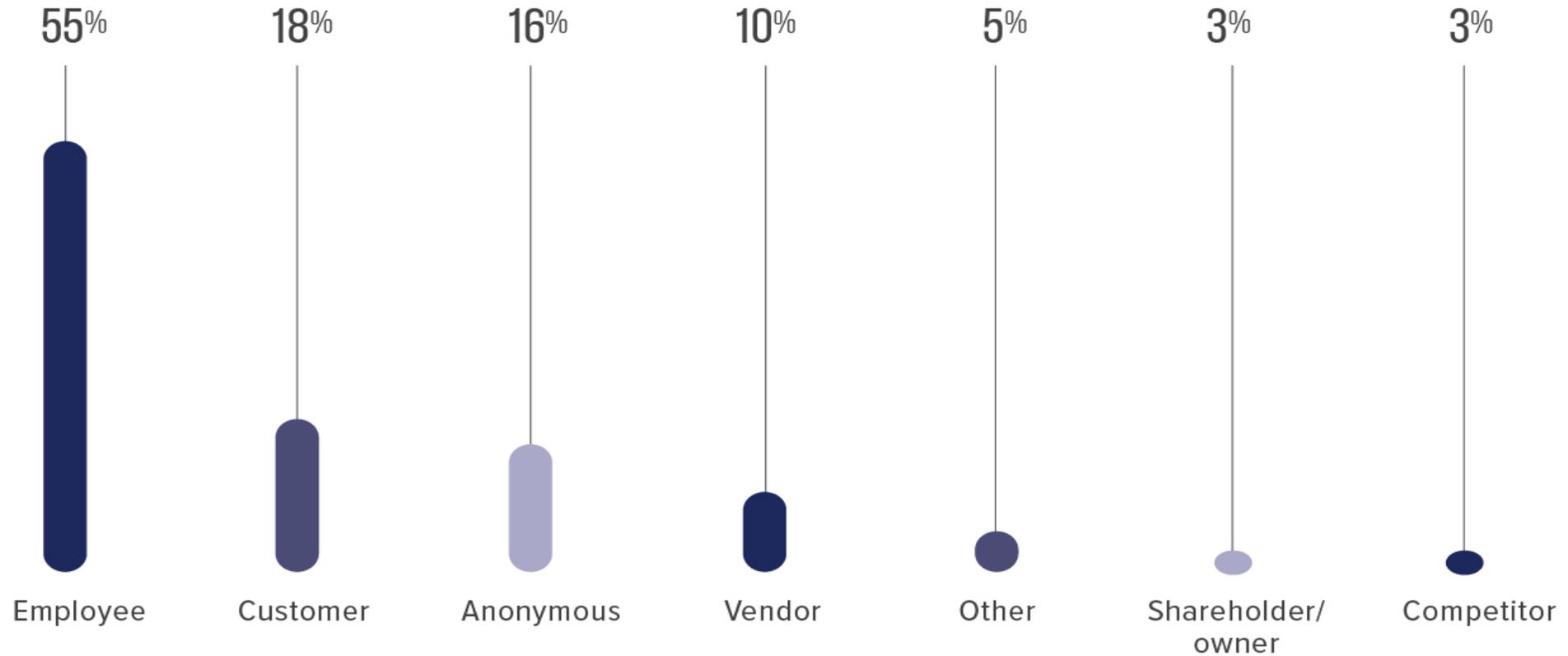
Former Texas College financial aid director indicted for alleged fraud

- A former director of financial aid at Texas College in Tyler is among those who have been indicted by a federal grand jury for student financial aid fraud on Nov. 16, 2022, according to the U.S. Attorney.
- Between August 2019 and February 2020, Angela Speech allegedly used her position as director of financial aid for Texas College to send financial aid payments to her son Jeremey Marshall and two others Devonaire Jones, 35, and Camyl Lewis, 24. (not eligible to receive aid)
- Speech and the three students worked together to knowingly misapply, steal and forge property provided and insured under federal subsidized and unsubsidized loan programs.
- The defendants face up to five years in federal prison if convicted.

HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED?



WHO REPORTS OCCUPATIONAL FRAUD?



Fraud in Higher Education...

BREAKING

HEADLINES

Baton Rouge man who masterminded \$1.8M student loan scam gets 11 years in federal prison

(January 2023)

- A Baton Rouge man who swiped the identities of 180 students and used their information to apply for student loans in their names, stealing more than \$1.8 million in financial aid from the government, is heading to federal prison.
- According to court documents, Elliot Sterling Jr. organized an elaborate scheme to defraud the U.S. Department of Education out of federal student loans and grants by masquerading as 180 purported students at Baton Rouge Community College and electronically submitting Free Applications for Federal Student Aid, or FAFSAs.
- Sterling acquired the students' private and personal information, then used it to fill out the FAFSA student loan applications, and sign master promissory notes leaving the victims on the hook to repay the loans.
- The group of students he enrolled into classes at the school included at least two inmates incarcerated in state prisons at the time and 145 students who didn't even have high school diplomas or GEDs.
- He falsified the qualifications for many of the students, submitting fake transcripts and bogus diplomas to the Department of Education to support his false claims. About 150 of the students listed "Sterling" as their mother's maiden name as the answer to a security question on federal student loan applications.
- Sterling had the student aid funneled into a personal bank account and used it to splurge on himself. Prosecutors said he spent more than \$250,000 of the defrauded dollars at casinos across the country.
- Evidence that prosecutors presented at trial proved Sterling raked in more than \$1.4 million in financial aid payouts.

https://www.theadvocate.com/baton_rouge/news/courts/baton-rouge-man-gets-11-years-for-18m-student-loan-scam/article_036626f0-9109-11ed-a1c5-4fd3c332b2ba.html

How Fraud Can Affect HCC...



Financial loss is generally the main effect of FRAUD in Higher Education, but...



Reputational Damage is another significant risk of Fraud in Higher Education. The Institution receiving...

- Negative publicity (i.e. news broadcasts, newspapers, rating agencies, etc.)
- Potential drop in future enrollment
- Potential drop in future advancement/development contributions

FRAUD TRIANGLE

Why Do People Commit Fraud?

The most widely accepted explanation for why some people commit fraud is known as the Fraud Triangle. The Fraud Triangle was developed by Dr. Donald Cressey, a criminologist whose research on embezzlers produced the term “trust violators.”



The Fraud Triangle hypothesizes that if all three components are present — unshareable financial need, perceived opportunity and rationalization — a person is highly likely to pursue fraudulent activities.

Fraud Triangle...

Perceived Pressure – a perceived, usually unshareable, financial need on the part of the fraud perpetrator.

- A person may be liable for significant liabilities, such as the cost of supporting sick relatives, college loans, car loans, and so forth.
- Or, they may have an expensive habit that requires ongoing funding.
- When the individual sees no way out of the situation, they may resort to fraud.
- However, there may only be a perceived level of pressure, such as earning comparatively less than one's friends.
- This latter situation can trigger expectations for a better lifestyle, perhaps involving a sports car, foreign travel, or a larger house.
- When a person does not see a clear path to meeting these expectations by honest means, he or she may resort to dishonest alternatives.

Fraud Triangle...

Opportunity - circumstances that allow fraud to occur

- When the preceding pressures are present, a person must also see an opportunity to commit fraud.
- For example, a maintenance worker may realize that there are no controls over checking out and returning tools; this is an opportunity for theft.
- Generally, the opportunity for fraud increases when a business has poor [internal controls](#).

Fraud Triangle...

Rationalization - an individual's justification for committing fraud

- An additional issue that is needed for fraud to continue over a period of time is the ability of the perpetrator to rationalize the situation as being acceptable.
- For example, a person stealing from a company's petty cash box might rationalize it as merely borrowing, with the intent of paying back the funds at a later date.
- As another example, a management team adjusts reported earnings for a few months during mid-year, in the expectation that sales will rise towards the end of the year, allowing them to eliminate the adjustments by year-end.



MOST COMMON BEHAVIORAL RED FLAGS OF FRAUD



When a person is engaged in occupational fraud, that person will often display certain behavioral traits that tend to be associated with fraudulent conduct.

Domineering / abusive style

Wheeler-dealer attitude

Unusually close association with a vendor or customer

Excessive control issues or unwillingness to share duties

Sudden change in lifestyle

Living beyond one's means

Dramatic change in financial stability

Fraud in Higher Education...



BREAKING

HEADLINES

Ex-Texas Southern adjunct instructor charged with stealing \$600K in fraudulent student loans

- A former Texas Southern University employee faces seven federal charges alleging that he fraudulently obtained \$600,000 in financial aid by enrolling "students" in Texas colleges and universities and submitting their loan applications for personal gain.
- Emmanuel Finnih, a 39-year-old from Richmond, is accused of using the fraudulent or stolen identifiers of 32 alleged students to obtain their financial aid.
- He allegedly enrolled the students at eight institutions: Houston Community College, Lone Star College, Texas Southern University, Blinn College, Tarrant County College District, Wharton County Junior College, Lee College and Austin Community College. Most of them did not attend, and they either failed or were withdrawn from their courses.
- Since 2017, Finnih used others' personal identifiers to prepare, submit and sign financial aid applications and master promissory notes in their names, authorities allege in the indictment. He also used mailing addresses, telephone numbers and email accounts he controlled to make sure communications and funds went directly to him, according to the charges filed by the attorney's office's Southern District of Texas.
- He obtained the financial aid refunds by way of electronic transfer, check and prepaid debit cards – in all, costing the U.S. over \$595,000, federal federal attorneys say.
- Finnih is also accused of stealing the identities of two alleged students. He and other unidentified individuals, who aided him in the process, used other people's documents in some of the applications, such as temporary driver permits or ID cards, according to the indictment.
- At least one of the stolen identities was from a person who was incarcerated at the time Finnih was accused of submitting false FAFSA forms. He sometimes altered women's names to appear masculine so he could use his own photos in the applications, authorities say.
- If convicted of theft of government funds, Finnih faces up to 10 years in federal prison. The aggravated identity theft charges carry two-year sentences, which must be served consecutively. The student financial aid fraud and unlawful use or transfer of identity documents each carry five-year prison terms.

<https://www.houstonchronicle.com/news/houston-texas/crime/article/richmond-man-600K-federal-fraud-student-loans-17483341.php>

WHAT ARE THE PRIMARY INTERNAL CONTROL WEAKNESSES THAT CONTRIBUTE TO OCCUPATIONAL FRAUD?



Fraud Risk Management

Create and maintain an environment where:

- The likelihood of fraud and other wrongdoing is minimized.
- Incidents that do occur are detected promptly.
- Incidents are handled efficiently and effectively.

6 Critical Actions to Help Reduce Fraud

1. Visible & Vocal Leadership – At Every Level

2. Policies on Fraud Responsibilities

3. Active Ongoing Fraud Risk Assessments

4. Anti-Fraud Controls

5. Anti-Fraud Daily Behaviors

6. Anti-Fraud Employee Skills Training

Visible & Vocal Leadership – At Every Level

Leaders At All Levels Must Talk About What They Expect

- Every employee must be recruited into anti-fraud efforts.
- Tell them how to think about fraud and the impact on their work.
- Tell them how this work will benefit them.

Nothing Meaningful Happens & Is Sustained Without Visible, Vocal Leadership!

HOW LEADERS CAN CREATE ETHICAL WORKPLACES

An organization's culture and ethics play a big role in how employees act. Leaders should create a culture that will positively influence employees and prevent negative associations to their workplace. Below are things every leader should focus on to create a positive ethical environment for employees:

•Ethics Training

- Make sure to have ethical policies, procedures and training in place.

•Whistleblower Policies

- Have a solid whistleblower policy in place that includes multiple avenues of reporting and an anti-retaliation policy.
- This helps employees be your eyes and ears to fraud and lets potential fraudsters know they can be caught and reported.

•Open-Door Policies

- Make sure employees know they have someone to talk to about ethical concerns and personal and professional problems.

•Reasonable Goal Setting

- Set aggressive but realistic targets for work.
- Gather feedback from involved employees to make sure they are realistic.
- Revisit goals to continually monitor if they're attainable.

•Be a Role Model for Positive Ethics

- Talk through potential situations to show employees how to handle them.
- Let them know that you also grapple with ethical considerations and reinforce the importance of seeking out guidance.

•Get Comfortable About Ethics

- Talk about ethics openly and nonjudgmentally.
- Make sure it is a subject everyone feels comfortable talking about on a day-to-day basis.



In virtually every business ethics or fraud case,
someone knew or strongly suspected BUT
STAYED SILENT!!



Why People Don't Speak Up

- It's none of my business
- It's not my job!
- There's no upside for me – only problems
- I won't fit in anymore
- Schoolyard mindset
- Fear – real or imagined
- They have never been asked to do so



**See something.
Say something.**

HCC is pleased to provide a third-party Ethics and Compliance Hotline for employees, students, and members of the public to encourage the reporting of any fraud, waste, and abuse and violations of College District policy and law.

<http://www.hccs.ethicspoint.com/>

1.855.811.6284



You Are HCC's MOST IMPORTANT Control in
Preventing Fraud!

HCC Policies on Fraud Responsibilities

BBFB (LEGAL)
CAK (LEGAL)
CDC (LOCAL)
CDE (LOCAL)
DGBA (LOCAL)
DH (LOCAL)
FEA (LOCAL)
FLB (LOCAL)
FLD (LOCAL)



Fraud Risk Assessments

Process to identify where fraud may occur and who may be committing it



Ask how would I
commit the
fraud?



Document the
controls in place
to prevent this
fraud from
happening.

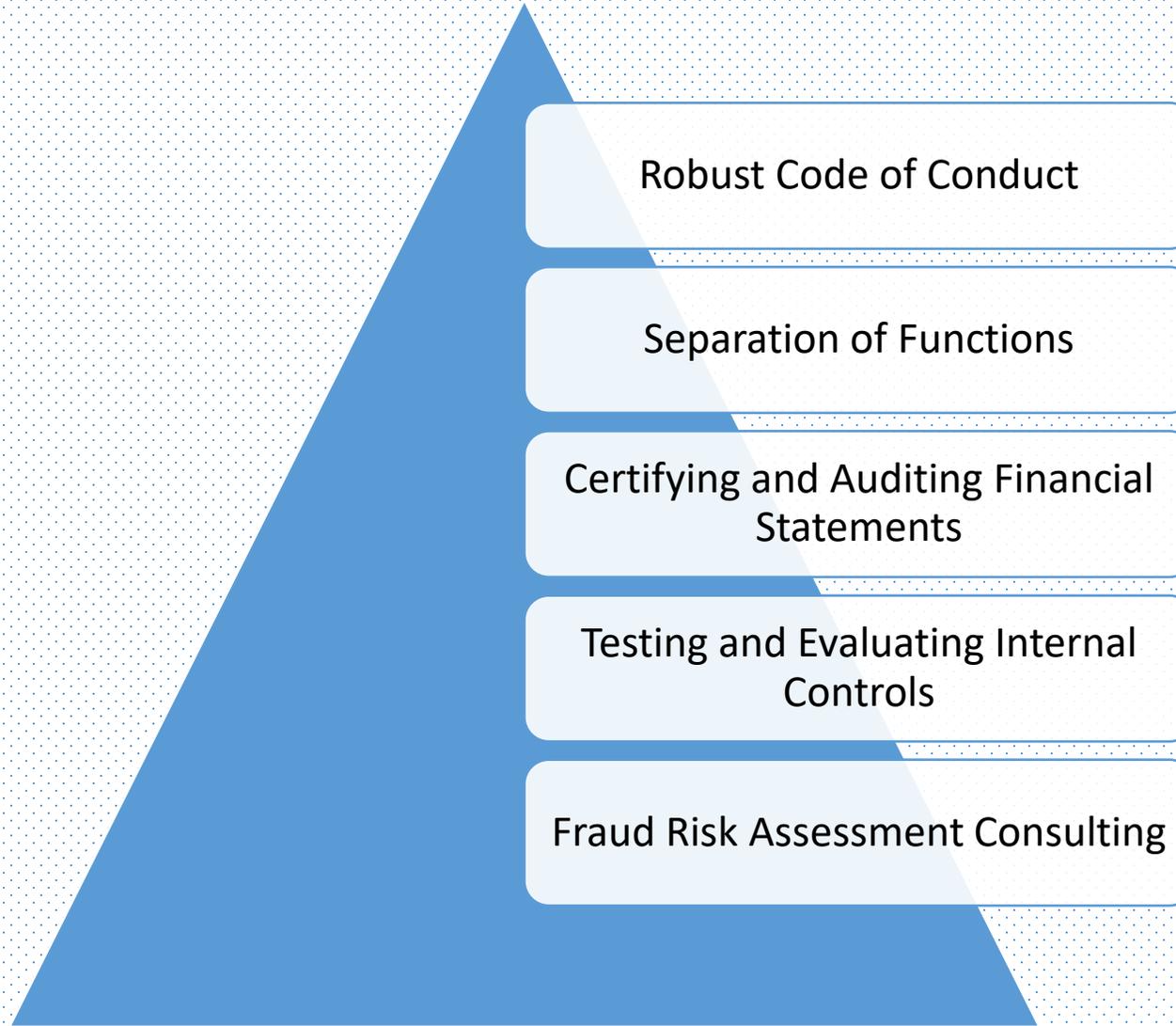


Determine
whether the
control
environment is
adequate to
prevent the fraud.



Add practical
procedures to
bring the control
environment to
an acceptable
level if needed.

Anti-Fraud Controls/Internal Controls

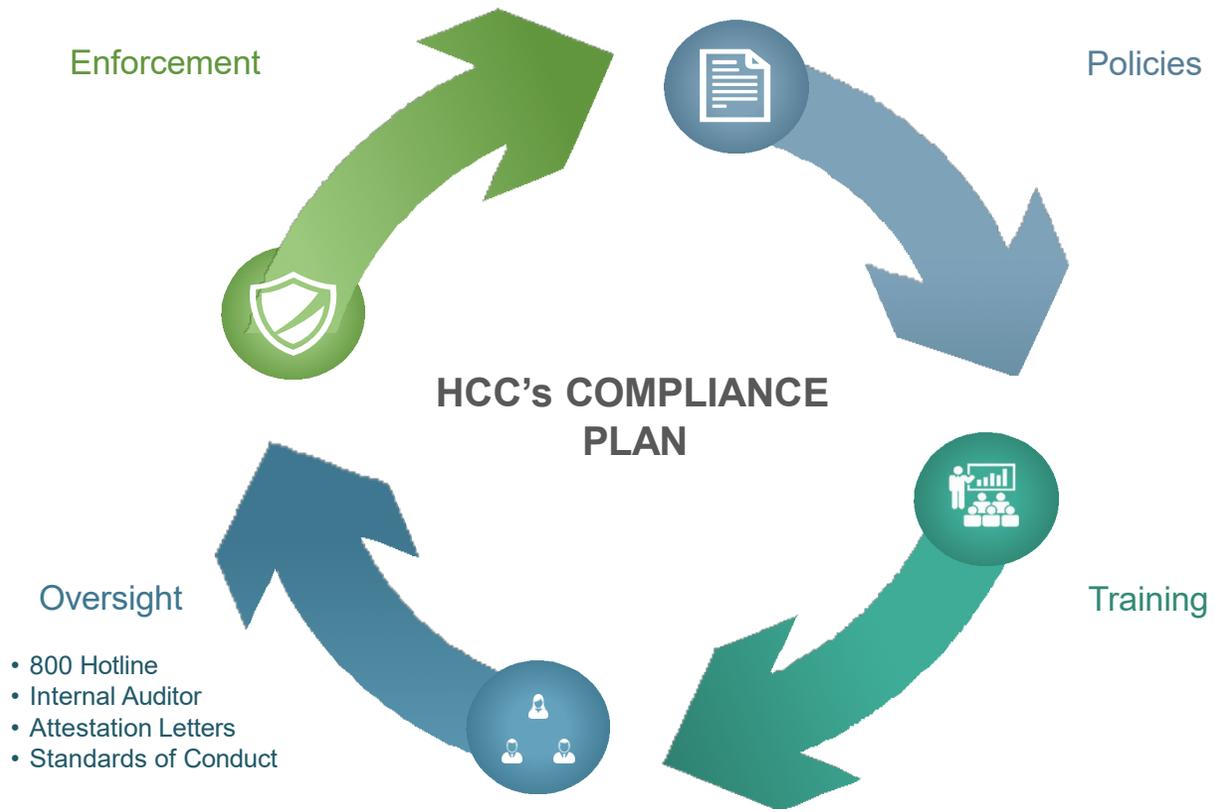


Anti-Fraud Employee Skills Training

HCC has mandatory annual training for ALL EMPLOYEES - Employee Standards of Conduct.

FRAUD SKILLS TO BE OBTAINED THROUGH TRAINING:

- General knowledge of fraud risks
- What can happen in their areas
- What it looks like in documents, reports and behaviors they see
- Suggestions on prevention
- Suggestions on prompt detection when prevention fails
- What to do with suspicions



Ransomware

What is it?

How does it happen?

In the Headlines...MGM casino hack

What is Ransomware?

- Ransomware is a type of criminal, money-making malware that uses encryption to “hijack” electronic files and systems. Bad actors (also known as hackers) trick users into clicking on deceptive links using social engineering tactics, and the ransomware locks files. Then the bad actor demands payment from the organization (the victim) before “releasing” the files to the owner and granting access.
- In a bad actors’ perfect-world scenario, once the ransom is paid, a decryption key is sent to the victim to allow system restoration, with the “promise” of no further harm. Unfortunately, however, in truth, paying the ransom is no guarantee the decryption key will be sent.

Types of Ransomware

There are two primary types of ransomware:

1. Locker — Blocks the victim's access to files but still allows for activities, including answering emails, and of course, paying ransoms.
 2. Crypto — Allows the victim to see their files and systems but not access them. This type is also known as “unlock locker ransomware.”
- Some crypto ransomware attacks include extortion (e.g., “Pay me \$XXX.XX or else!”).
 - Criminals can also purchase Ransomware as a Service (RaaS) if they do not have the expertise to develop and/or attach ransomware themselves.

How does it
happen?

Ransomware attacks (exploitation) begin with a malicious payload that is accomplished via:

- Work that exploits a system/software weakness.
- An advertisement that directs to a website containing an exploit kit.
- A link or attachment that contains malicious software.
- An infected device being placed on the network.
- Social engineering and/or phishing email.
- Missing patches.

MGM Casino Hack

- MGM resorts said costs from a disruptive ransomware hack has exceeded \$110 million, including \$10 million in one-time consulting cleanup fees.
- MGM Resorts, which manages prominent hotels like Mandalay Bay (site of the Black Hat security conference), Bellagio, MGM Grand, Aria, Luxor and the Cosmopolitan.
- MGM Resorts said the hackers stole personal information (including name, contact information (phone number, email address and postal address), gender, date of birth and driver's license numbers).
- <https://www.kolide.com/blog/what-everyone-got-wrong-about-the-mgm-hack>

MGM Casino Hack continued...

- How did it happen?
- How did MGM respond?
- Public fallout and MGM's losses
- Was any customer information stolen?



Fraud in Higher
Education??

Would you consider this fraud??



At ACC, nearly \$500K in student pandemic aid went to employees

- Austin Community College launched an internal review of its aid distribution, determining that 115 full-time employees received nearly \$500,000 of pandemic grants intended to help struggling students.
- It was found that many of those employees were career staffers who were not taking course credit before, or after, the semester they enrolled and qualified for emergency student assistance.
- ACC staff that received HEERF money included a director-level employee earning over \$80,000 who received \$1,500 and a provost-office worker with a \$90,000 salary who got a \$3,500 grant. Neither of them took a course before or after the semester they signed up for classes and applied for grants.
- Also found nine workers in the financial aid office received HEERF money, including five who were involved in the handling of grant fund applications – which could include application approval, denial, awarding or processing, according to ACC.
- ACC did not comment on specific employees, courses or grants, but the college said its ongoing review has found that all disbursements of HEERF funds reviewed so far have complied with federal guidelines.
- However, one COVID-aid watchdog said the college’s use of the student aid raises troubling red flags.
- <https://www.kxan.com/investigations/at-acc-nearly-500k-in-student-pandemic-aid-went-to-employees>

- Terry Corrigan, Internal Audit Director
- 713-718-7278
- hcc.internalaudit@hccs.edu
- <https://www.hccs.edu/departments/internal-auditing/>



**See something.
Say something.**



Questions/Comments
(*use Panel Options "Q&A"*)

