

 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 13-19, 2022
- 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.



November 13-19, 2022

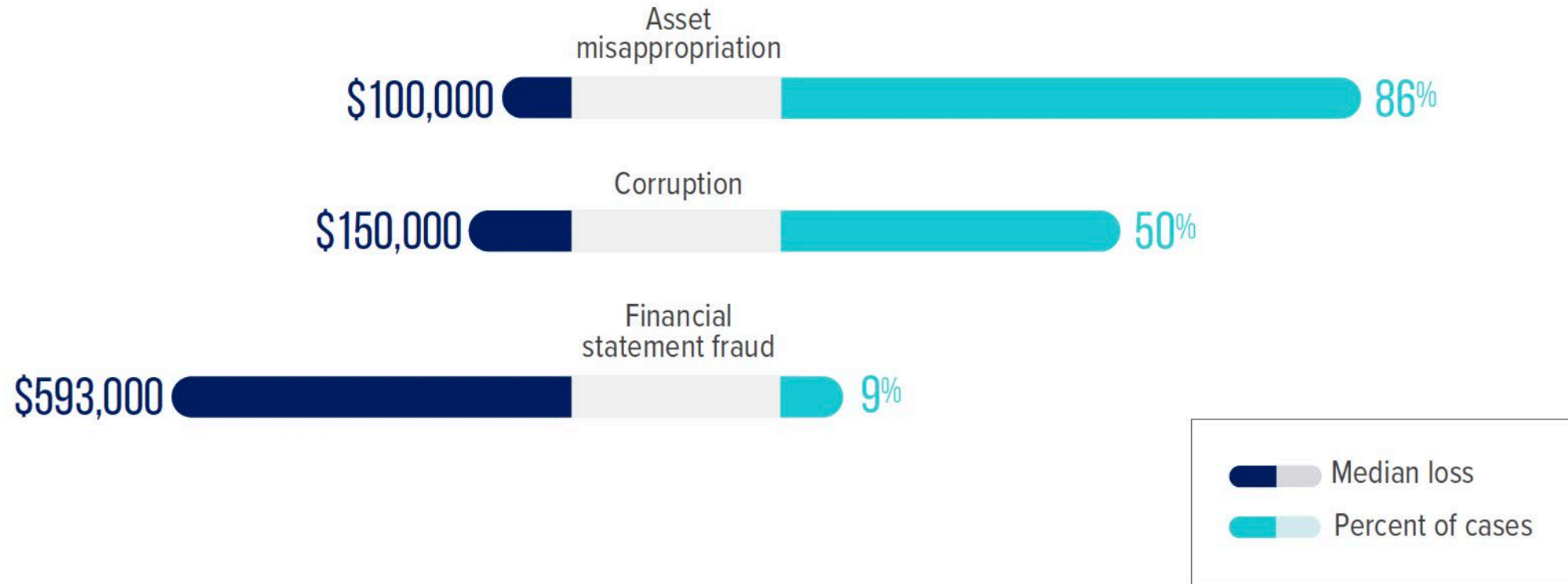
HOUSTON COMMUNITY COLLEGE

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?



HOW IS OCCUPATIONAL FRAUD COMMITTED?

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

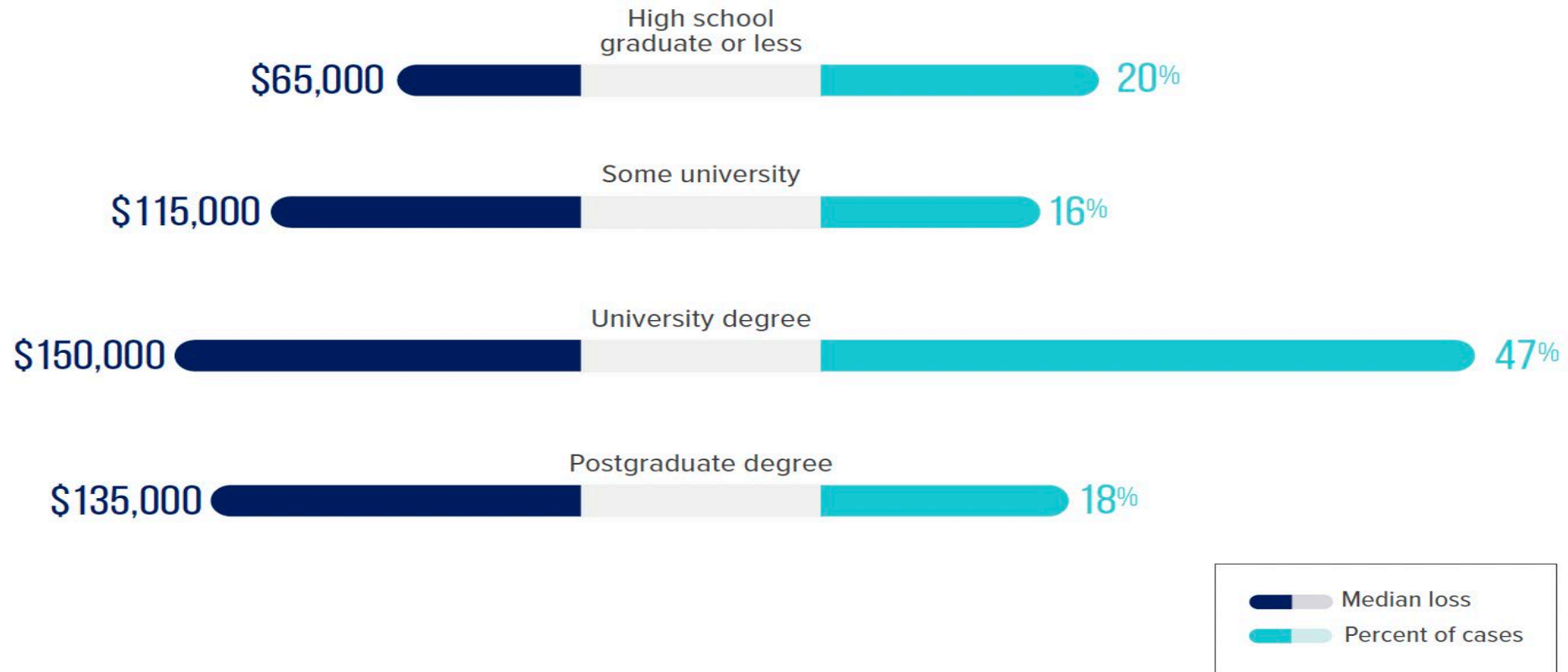
What does a “TYPICAL” Fraudster look like?



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



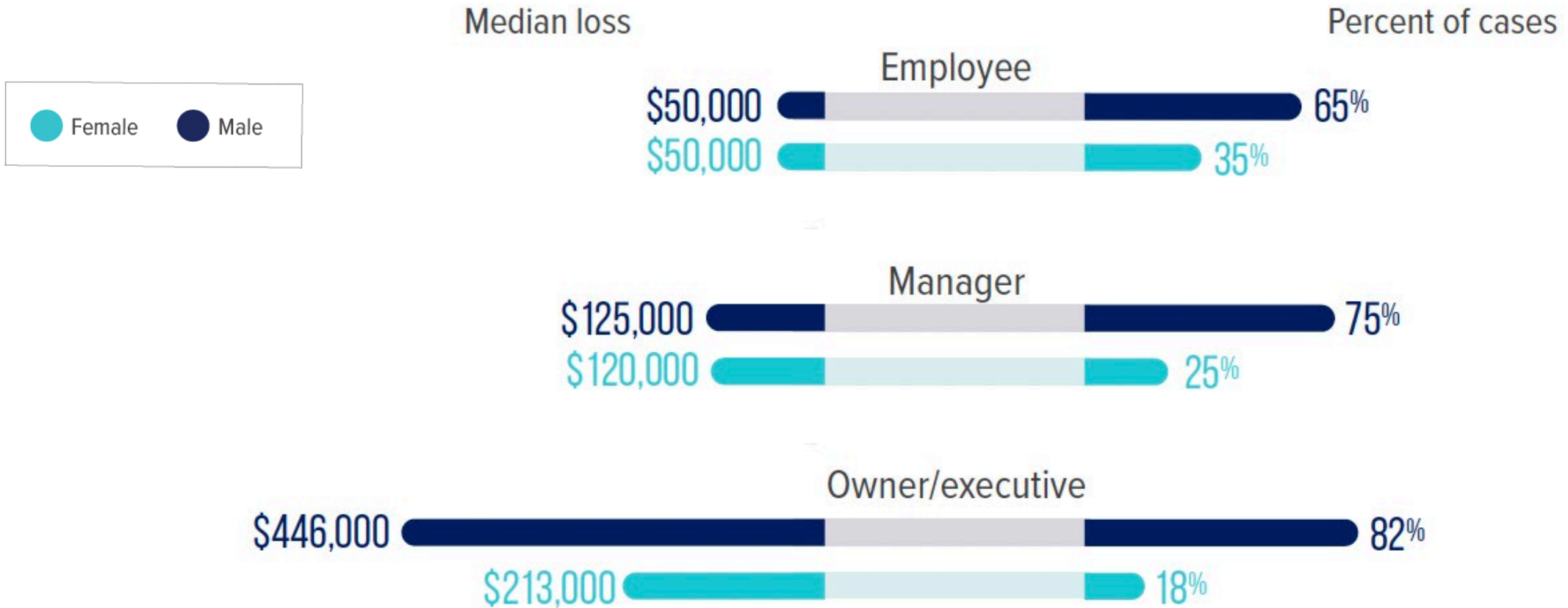
HOW DOES THE PERPETRATOR'S EDUCATION LEVEL RELATE TO OCCUPATIONAL FRAUD?



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?



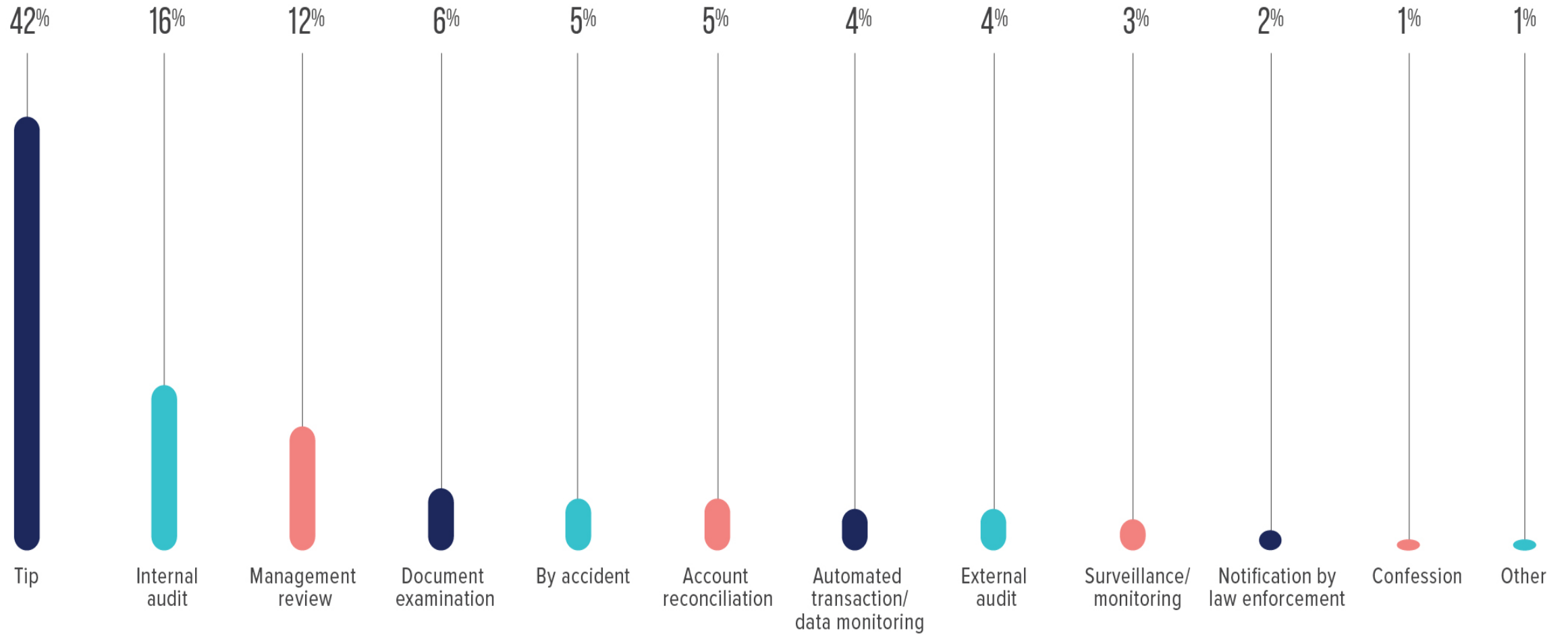
Fraud in Higher Education...



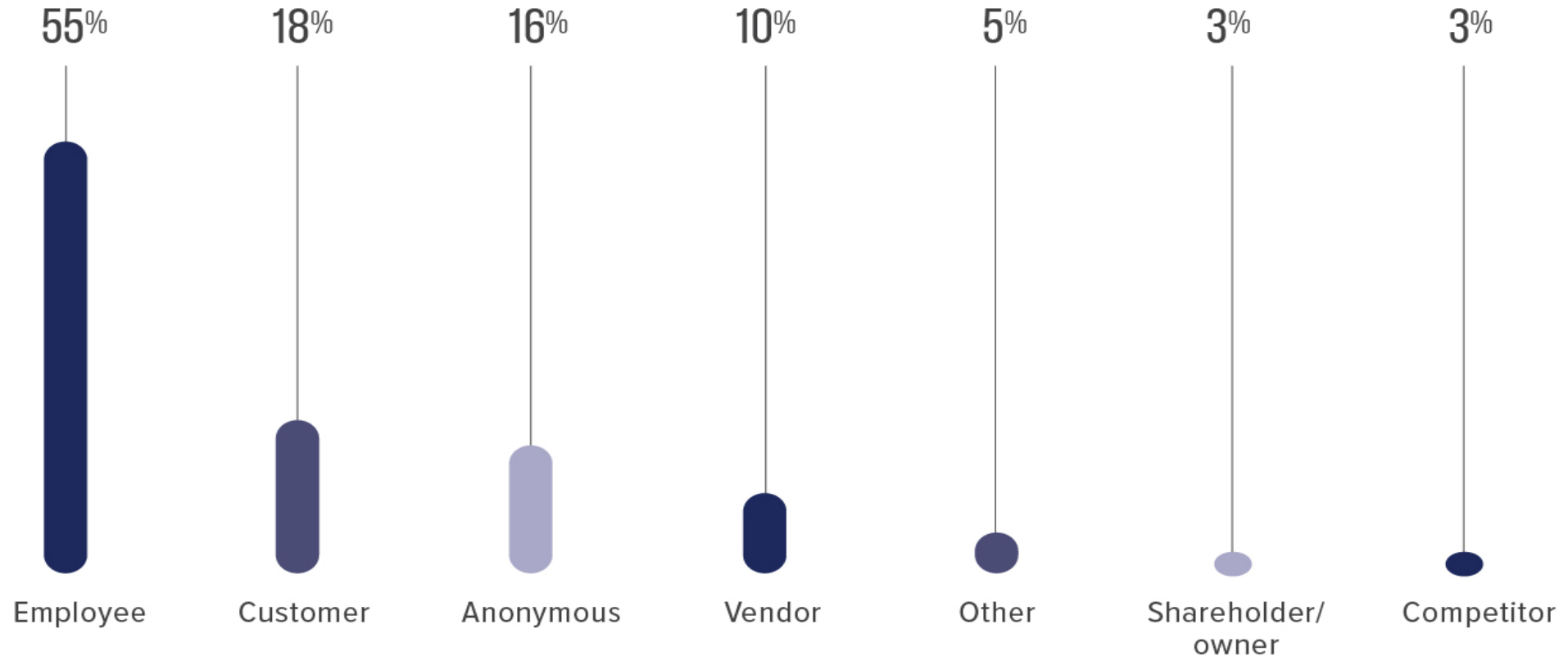
Local man indicted for student financial aid fraud

- HOUSTON – A 39-year-old Richmond resident charged with fraudulently obtaining nearly \$600,000 in financial aid funds at several Texas colleges and universities.
- 2017 through to present.
- Submitted false applications for financial aid.
- He unlawfully obtained financial aid funds for over 30 alleged students at eight colleges and universities in Texas.
- Used the personal identifiers of other individuals to prepare, submit and sign false and fraudulent financial aid applications and master promissory notes in their names.
- Utilized mailing addresses, telephone numbers and email accounts he controlled to ensure that the Department of Education and colleges would send any communications directly to him.

HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED?



WHO REPORTS OCCUPATIONAL FRAUD?



Most Common Fraud Schemes in Education

Of 69 cases reviewed related to Education...

- Billing – 26%
- Cash Larceny – 9%
- Cash on Hand – 12%
- Checking and Payment Tampering – 12%
- Corruption – 49%
- Expense Reimbursement – 12%
- Financial Statement Fraud – 12%
- Noncash – 19%
- Payroll – 14%
- Skimming – 12%

Fraud in Higher Education...



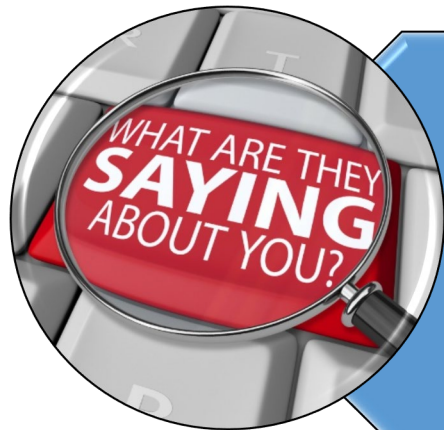
Richmond Community College Director Sentenced for Stealing Student Financial Aid Funds

- RICHMOND, Va. – A Richmond woman sentenced to 63 months in prison for orchestrating a six-year scheme to defraud the United States Department of Education and the Commonwealth of Virginia of at least \$230,000 in student financial aid funds.
- Kiesha Pope, 48, Director of Financial Aid (2006 – 2017) J. Sargeant Reynolds Community College.
- 2011 - 2017, Pope involved in a scheme to defraud the DOE, the Commonwealth of Virginia, and Reynolds.
- Pope used her financial aid office access to manufacture or boost financial aid eligibility for individuals, often her family members, who were not eligible for financial aid.
- Pope fraudulently overrode Reynolds' internal automated controls to manually place co-conspirators in a status that guaranteed their continued receipt of financial aid funds.
- Pope used her system access to procure financial aid for her son from 2011 through 2017; son was not attending Reynolds.
- Pope procured financial aid for her ex-fiancé who was actually serving a term of incarceration.
- Pope spent funds on her personal expenses, such as a vacation on Disney Cruise Line, shopping and expenses for her daughter.

How Fraud Can Affect HCC...



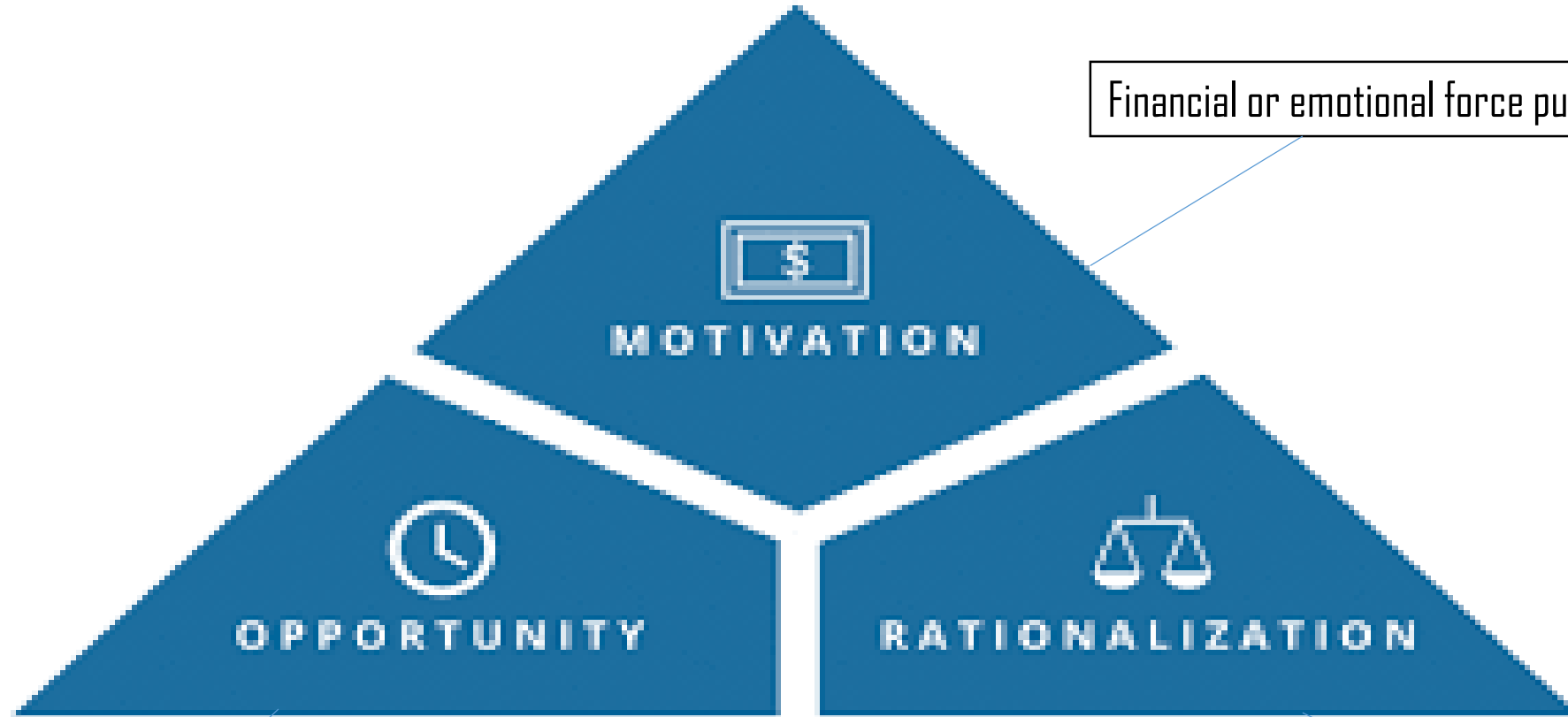
Financial loss is generally the main effect of FRAUD in Higher Education, but...



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



Financial or emotional force pushing towards fraud

Ability to execute plan without being caught

Personal justification for dishonest actions



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.

The eight most common red flags identified in the fraud cases reviewed in Report to Nations were:

(1) living beyond means;

(2) financial difficulties;

(3) unusually close association with a vendor or customer;

(4) excessive control issues or unwillingness to share duties;

(5) unusual irritability, suspiciousness, or defensiveness;

(6) bullying or intimidation;

(7) recent divorce or family problems; and

(8) a general “wheeler-dealer” attitude involving shrewd or unscrupulous behavior.

HOW DO PERPETRATORS CONCEAL THEIR FRAUDS?

Examining the methods fraudsters use to conceal their crimes can assist organizations in more effectively detecting and preventing similar schemes moving forward.

TOP 5 CONCEALMENT METHODS USED BY FRAUDSTERS



39%

Created fraudulent physical documents



32%

Altered physical documents



28%

Created fraudulent electronic documents or files



25%

Altered electronic documents or files



23%

Destroyed or withheld physical documents

12% of fraudsters don't even attempt to conceal the fraud

Fraud in Higher Education...



Former Bossier Parish Community College Comptroller Sentenced for Stealing More Than \$280,000

- **SHREVEPORT, La. - Carol Bates**, the former comptroller for Bossier Parish Community College (BPCC), was sentenced, for conspiracy to commit wire fraud, to 60 months (5 years) in prison and restitution in the amount of \$286,987.08.
- From 2013 to 2016, Bates used her position as comptroller of BPCC to access an internal BPCC computer database and make entries falsely showing individuals were due refunds by the school.
- The individuals were not qualified to receive the funds, and, in most cases, were not even attending BPCC.
- As a part of the scheme, Bates and her sister, Audrey Williams, recruited 9 individuals to receive fraudulent refunds from BPCC.
- Once the individual received the funds, they were instructed to deliver between one-half and two-thirds of the money to Bates or her sister.
- [Former Bossier Parish Community College Comptroller Sentenced for Stealing More Than \\$280,000 | USAO-WDLA | Department of Justice](#)

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



Easy Ways to Reduce Fraud Risk

Management
Controls/
Anti-Fraud
Controls

Fraud Risk
Assessments

Fraud Hotline

Anti-Fraud Controls



Robust Code of Conduct

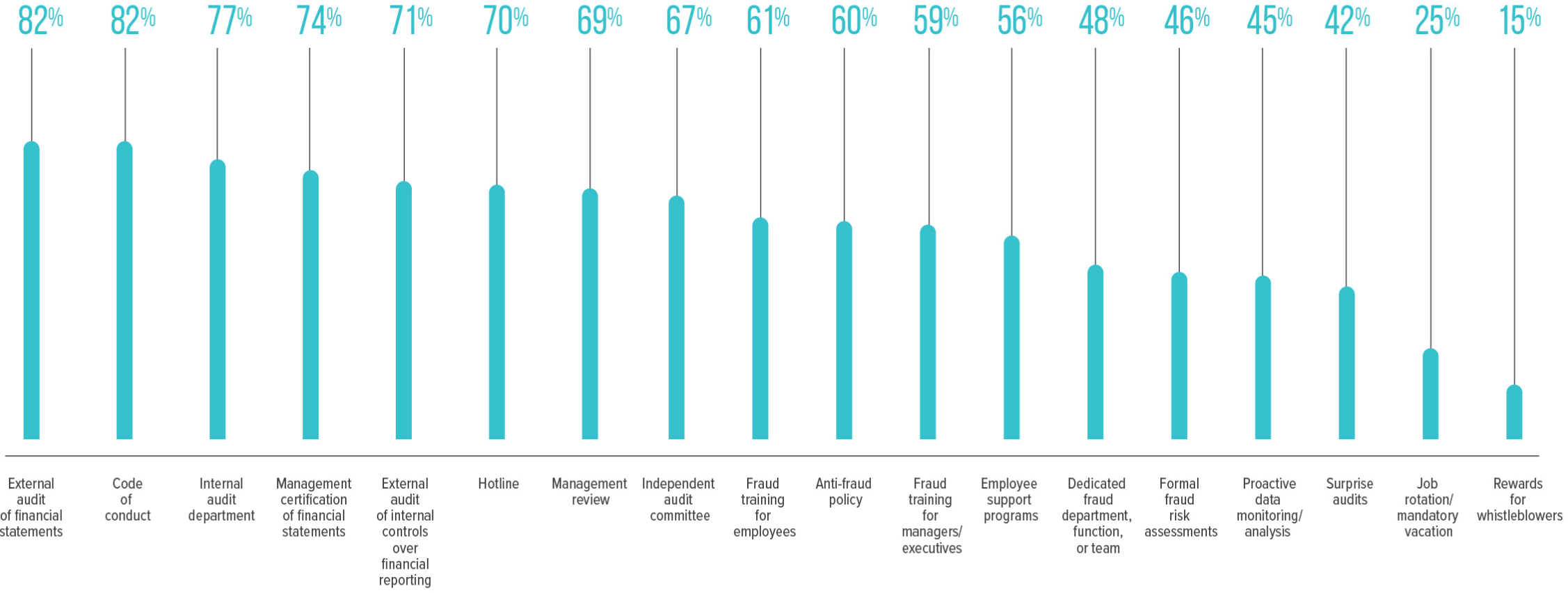
Separation of Functions

Certifying and Auditing Financial
Statements

Testing and Evaluating Internal
Controls

Fraud Risk Assessment Consulting

WHAT ANTI-FRAUD CONTROLS ARE MOST COMMON?



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.



**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

HOTLINE AND REPORTING MECHANISM EFFECTIVENESS

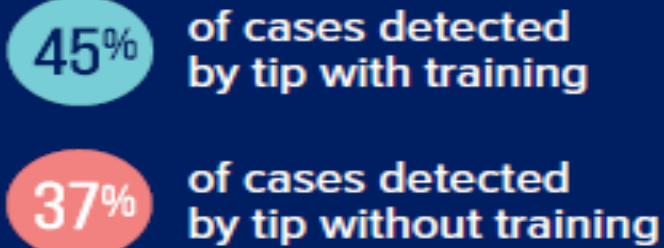
70% of
VICTIM
ORGANIZATIONS
had hotlines

Fraud losses were
2X HIGHER 
at organizations without hotlines

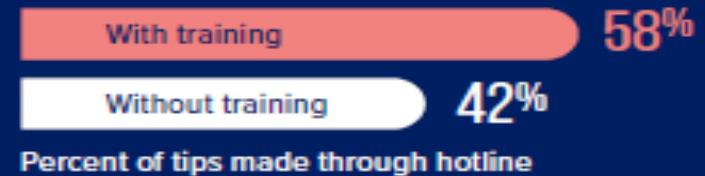


EFFECT OF EMPLOYEE AND MANAGER FRAUD AWARENESS TRAINING ON HOTLINES AND REPORTING

TRAINING INCREASES
the likelihood of detection by tip



Reports of fraud are
MORE LIKELY TO BE SUBMITTED
through hotlines
with training



Ransomware

What is it?

How does it happen?

In the Headlines...Ransomware in Education

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.

Florida School District

- Hackers who demanded up to \$40 million from a Florida School District for the keys to decrypt files. The Hackers later reduced the ransom to \$10 million.
- The malware group posted to a public website the 26,000 stolen files after the district announced it had no intention of paying a ransom.
- The files released contained names, dates of birth, and Social Security numbers.

HCC Policies on Fraud Responsibilities

- Policies

BBFB (LEGAL)

CAK (LEGAL)

CDC (LOCAL)

CDE (LOCAL)

DGBA (LOCAL)

DH (LOCAL)

FEA (LOCAL)

FLB (LOCAL)

FLD (LOCAL)



- Employee Standards of Conduct annual training is mandatory for all HCC employees

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



- 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"*)

