Understanding and Preventing Fraud in Higher Education

Presented by

HCC Internal Audit Department

November 20, 2024

International Fraud Awareness Week

INTERNATIONAL
FRAUD
AWARENESS
WEEK

November 17–23, 2024

November 17-23, 2024

Organizations worldwide lose an estimated 5 percent of their annual revenues to fraud, according to Occupational Fraud 2024: 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.

Questions/Comments

(*use Panel Options "Q&A"*)

What is Fraud?

The act of using dishonesty to obtain something of value or to deprive others of something of value.

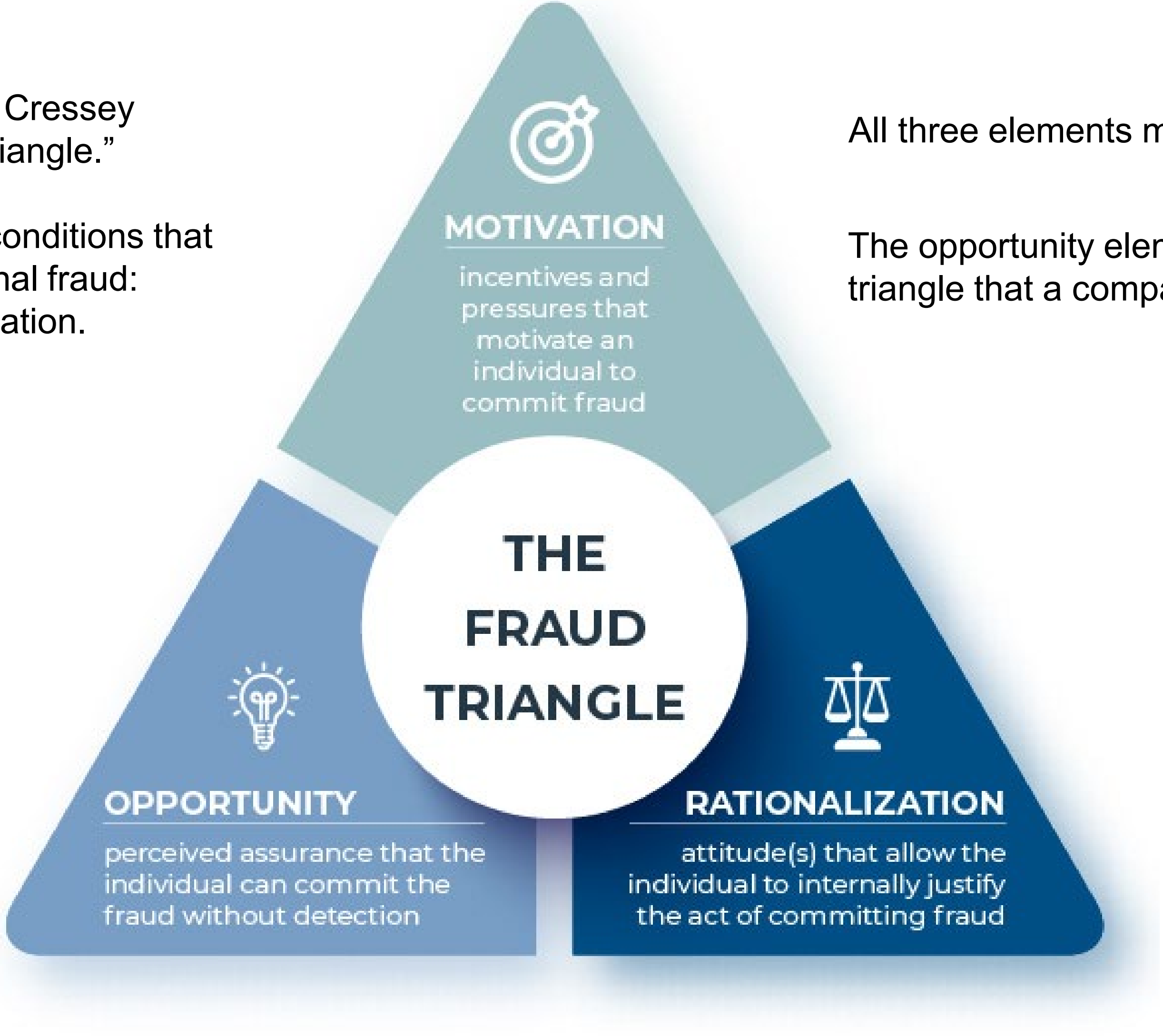
Fraud can include making false statements, concealing information, or misrepresenting facts.

Management has a responsibility for managing the risk of fraud.

FRAUD TRIANGLE

In the 1970s, criminologist Donald R. Cressey published a model called the “fraud triangle.”

The fraud triangle outlines the three conditions that lead to higher instances of occupational fraud: motivation, opportunity, and rationalization.



THE FRAUD TRIANGLE

MOTIVATION

incentives and pressures that motivate an individual to commit fraud

OPPORTUNITY

perceived assurance that the individual can commit the fraud without detection

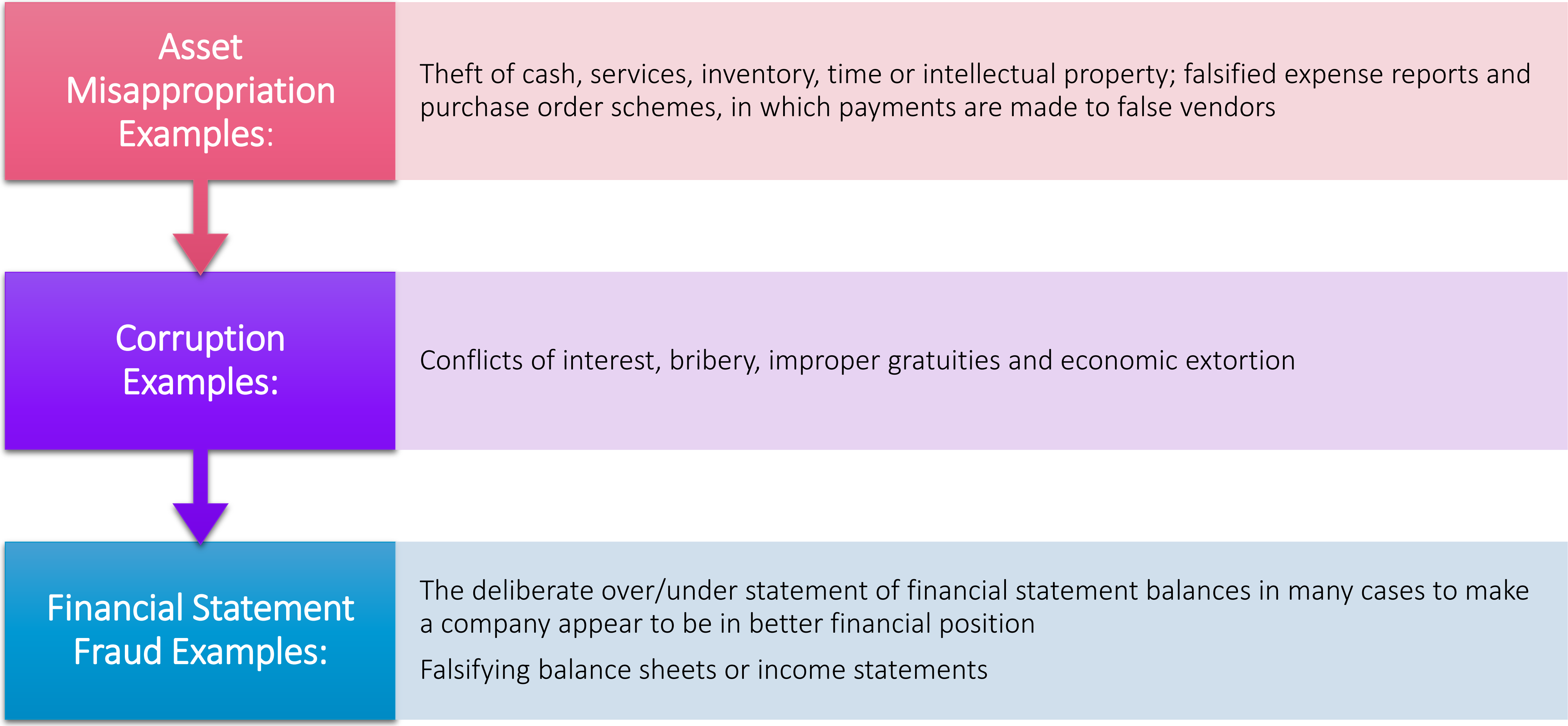
RATIONALIZATION

attitude(s) that allow the individual to internally justify the act of committing fraud

All three elements must be present for fraud to occur.

The opportunity element is the **only** part of the fraud triangle that a company can significantly control.

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

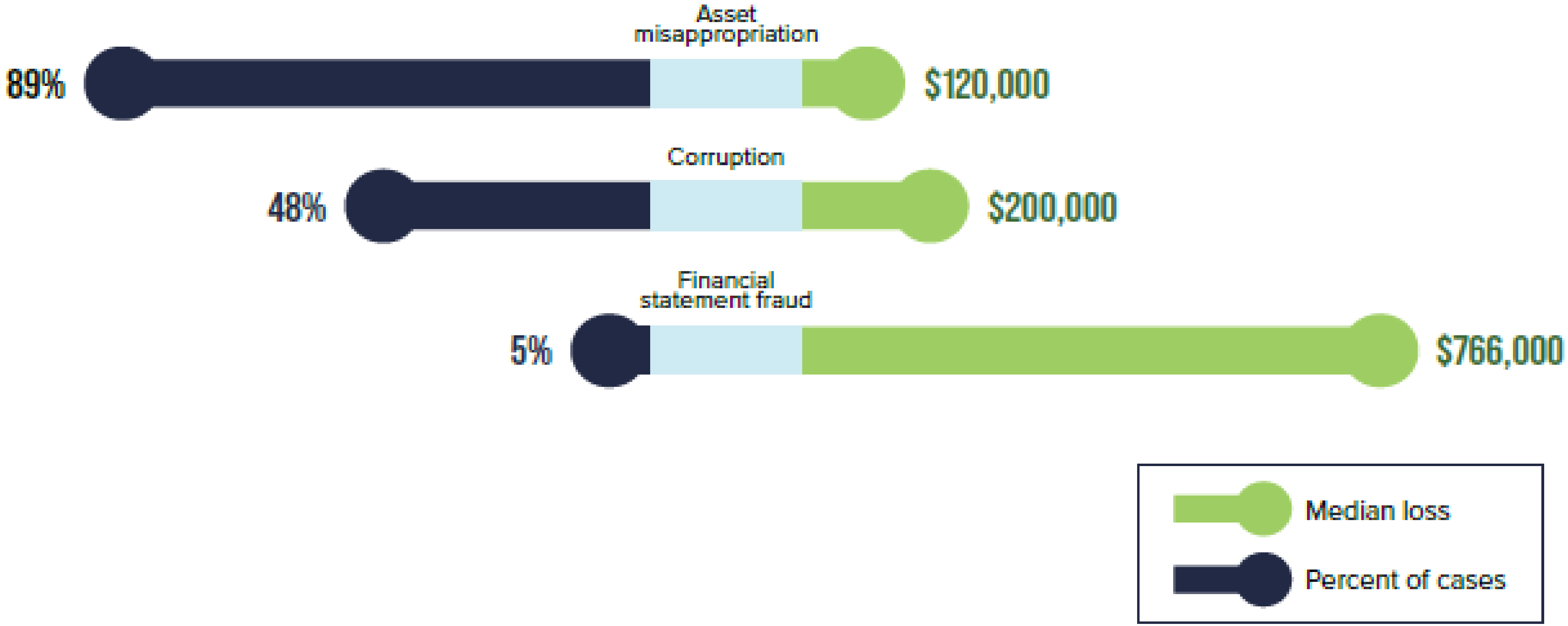
Falsifying balance sheets or income statements

Assoc. of Certified Fraud Examiners (ACFE) Report to the Nations 2024

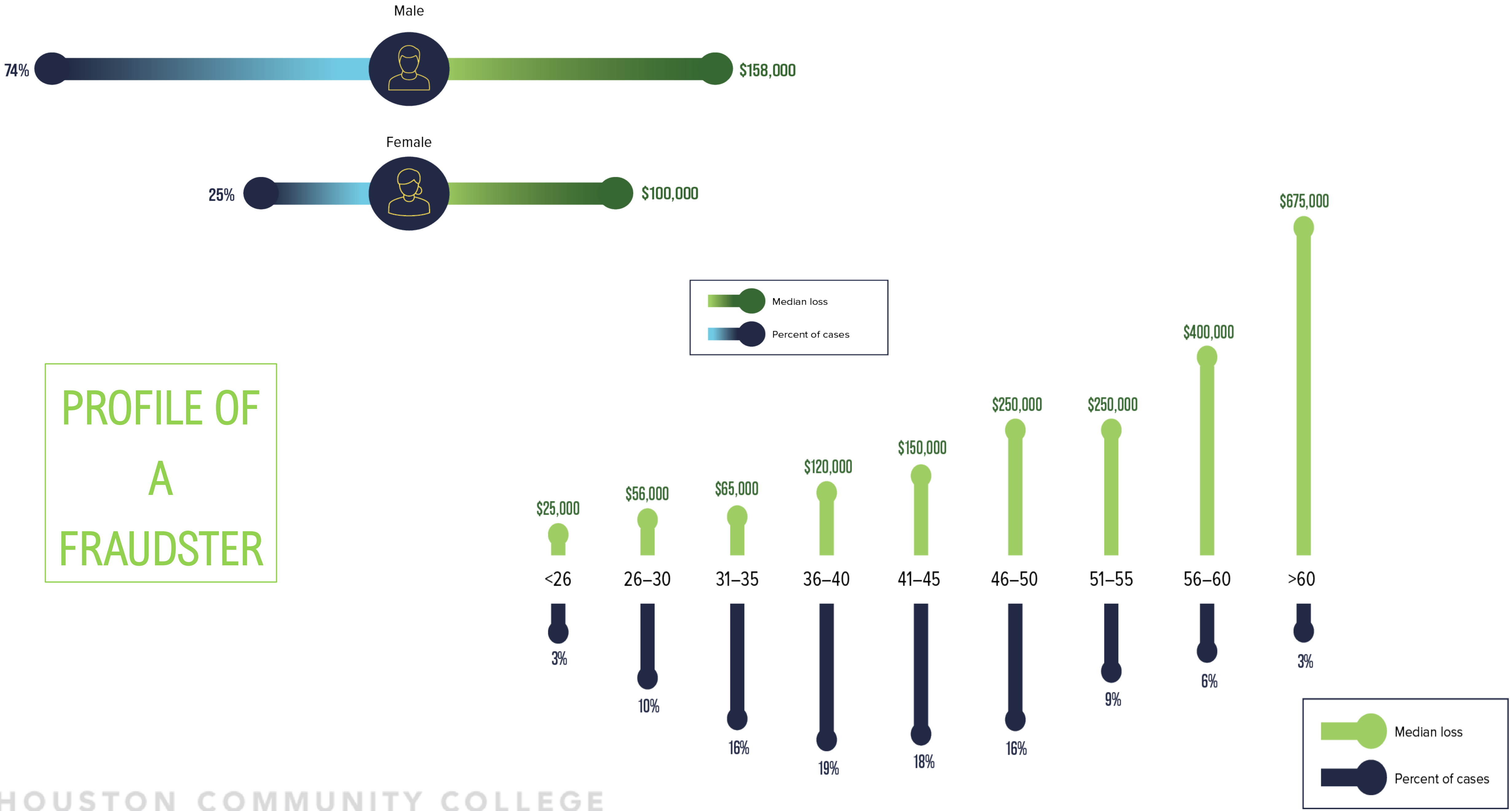
Key Findings - Based on 1,921 real cases of occupational fraud

HOW IS OCCUPATIONAL FRAUD COMMITTED?

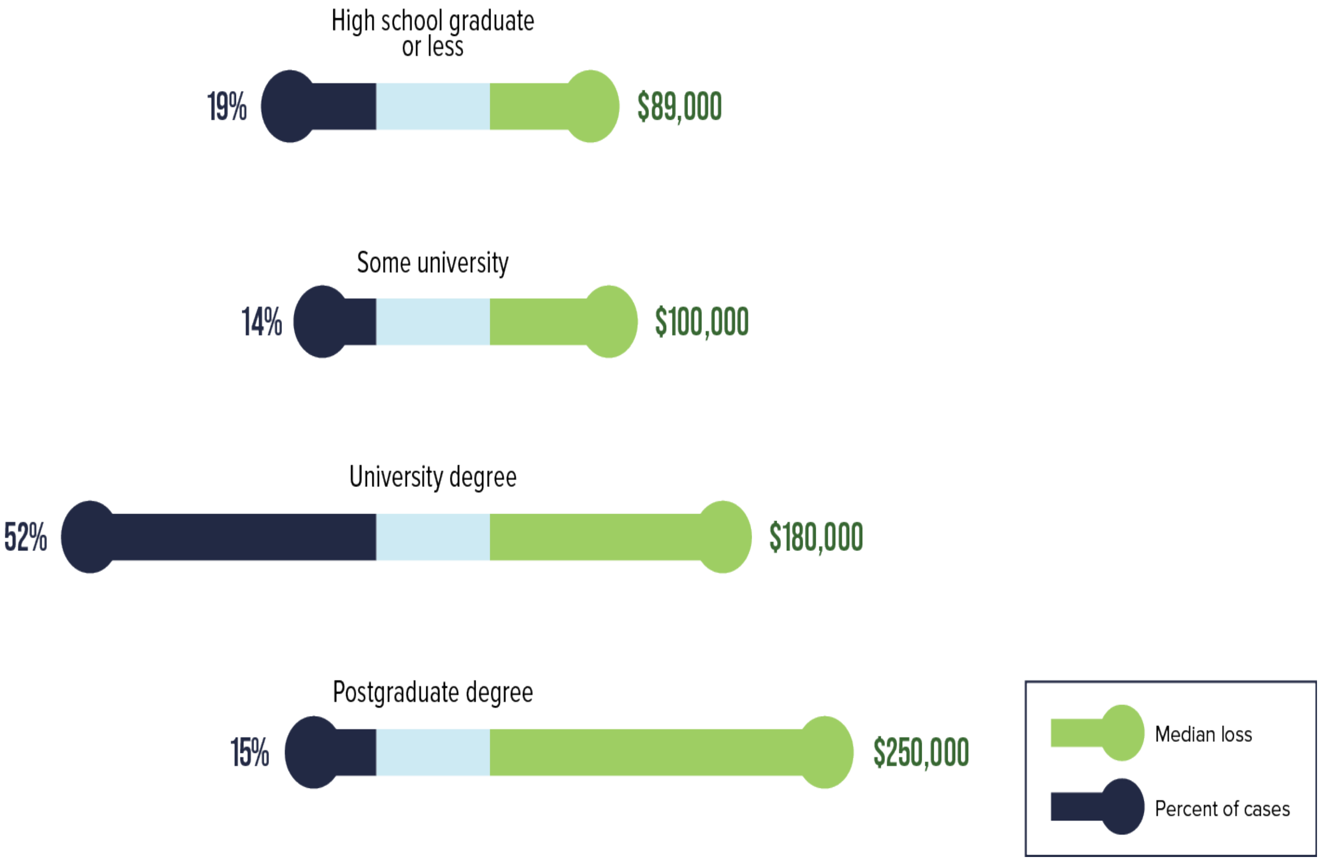
FIG. 2 HOW IS OCCUPATIONAL FRAUD COMMITTED?

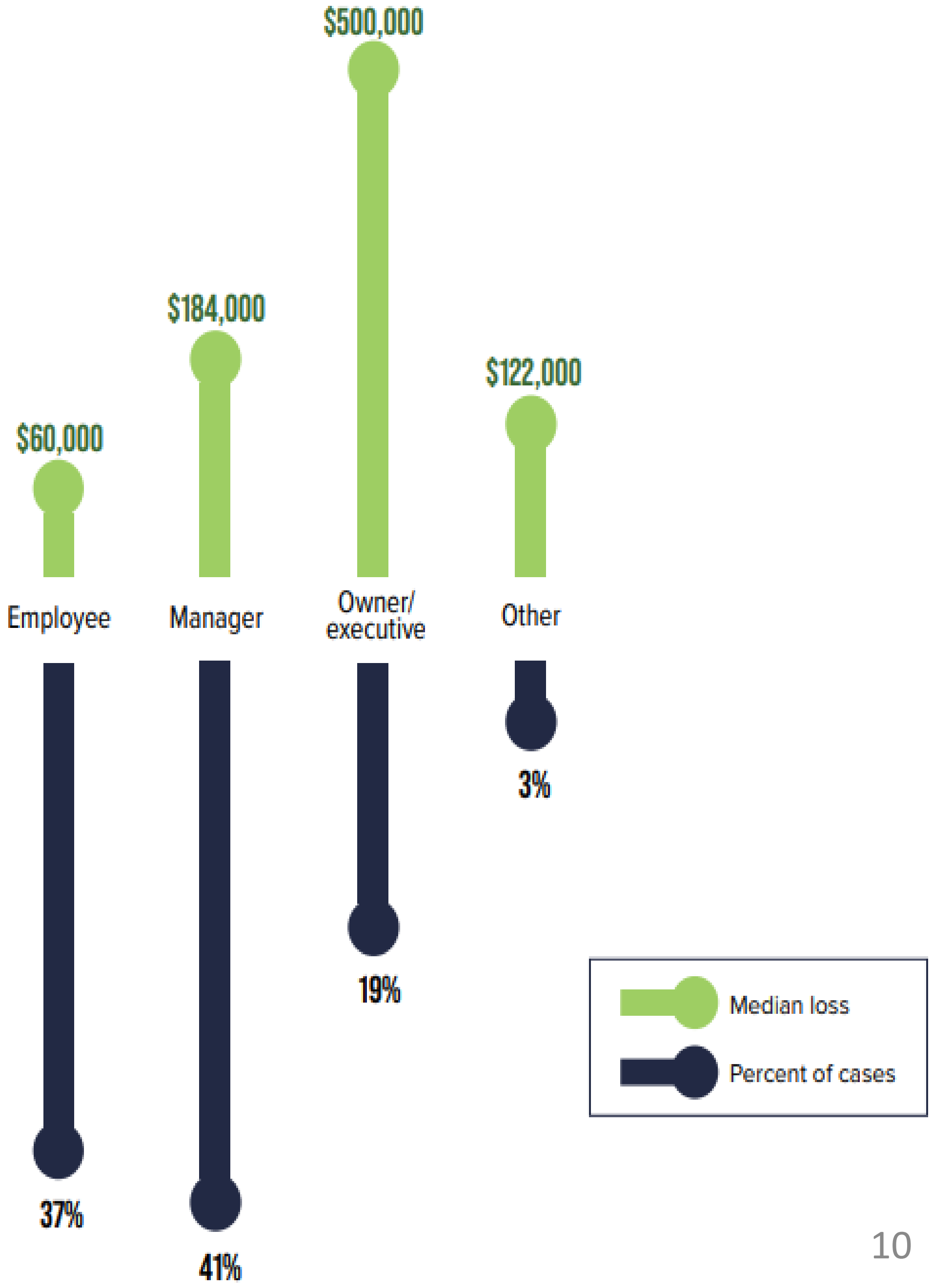


PROFILE OF A FRAUDSTER



PROFILE OF A FRAUDSTER





POLL QUESTION #1

Most common type of fraud in higher education?

1. Asset Misappropriation
2. Corruption
3. Financial statement fraud

POLL QUESTION #2

What do you think is median loss due to fraud in higher education institutions?

1. $1,000,000
2. $75,000
3. $50,000
4. $250,000

The Impact of Fraud on Higher Education

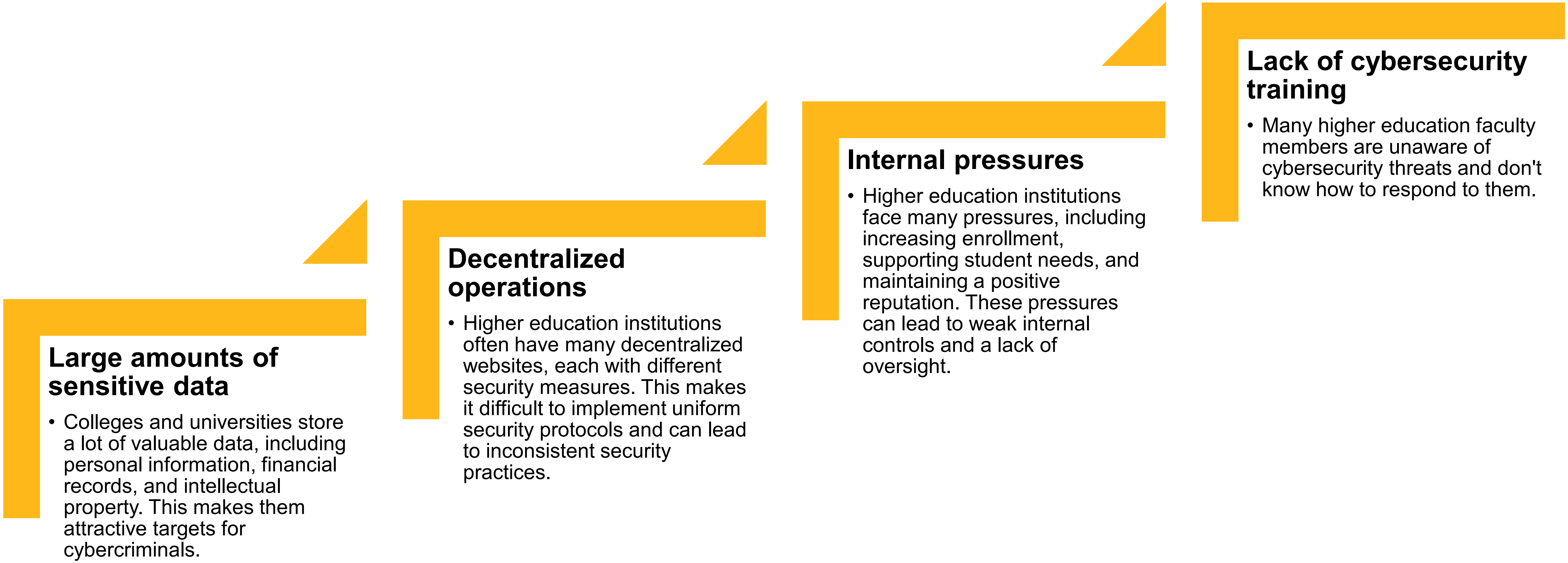
According to ACFE,
Report to the Nations 2024

The median loss due to fraud in educational institutions was $50,000.

The most common type of fraud in education was CORRUPTION.

(in 70 case studies related to education)

Why Higher Education Institutions are Vulnerable:



Large amounts of sensitive data

- Colleges and universities store a lot of valuable data, including personal information, financial records, and intellectual property. This makes them attractive targets for cybercriminals.

Decentralized operations

- Higher education institutions often have many decentralized websites, each with different security measures. This makes it difficult to implement uniform security protocols and can lead to inconsistent security practices.

Internal pressures

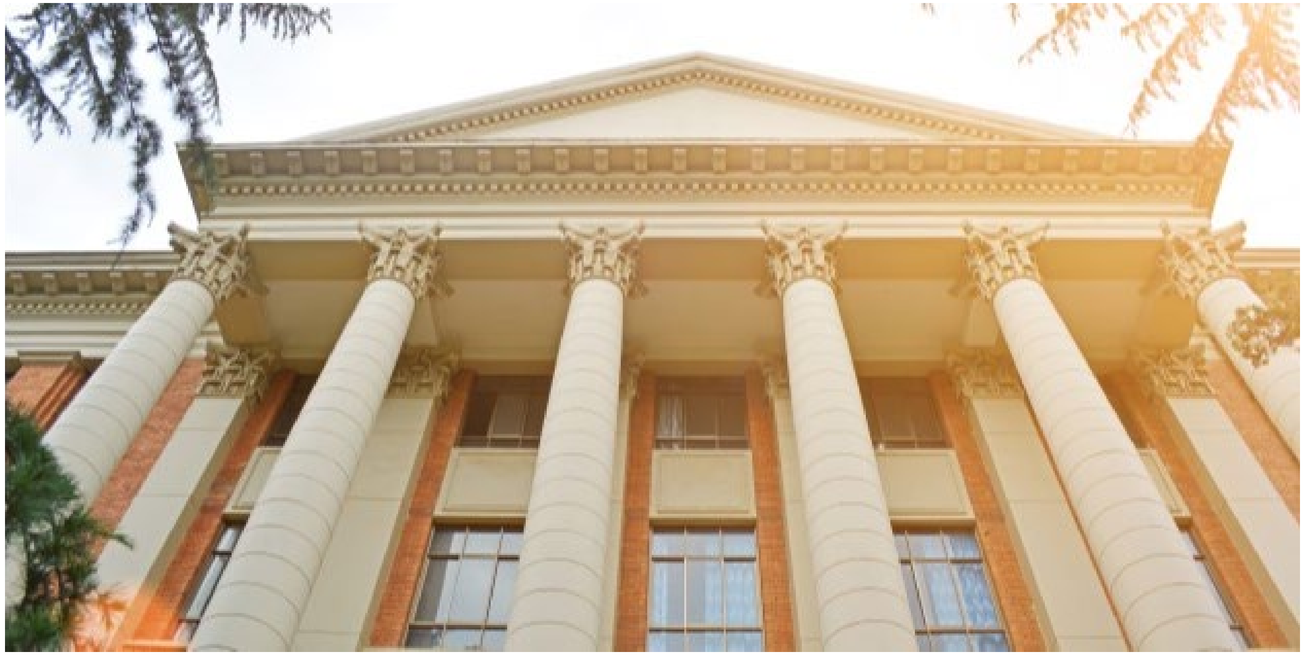
- Higher education institutions face many pressures, including increasing enrollment, supporting student needs, and maintaining a positive reputation. These pressures can lead to weak internal controls and a lack of oversight.

Lack of cybersecurity training

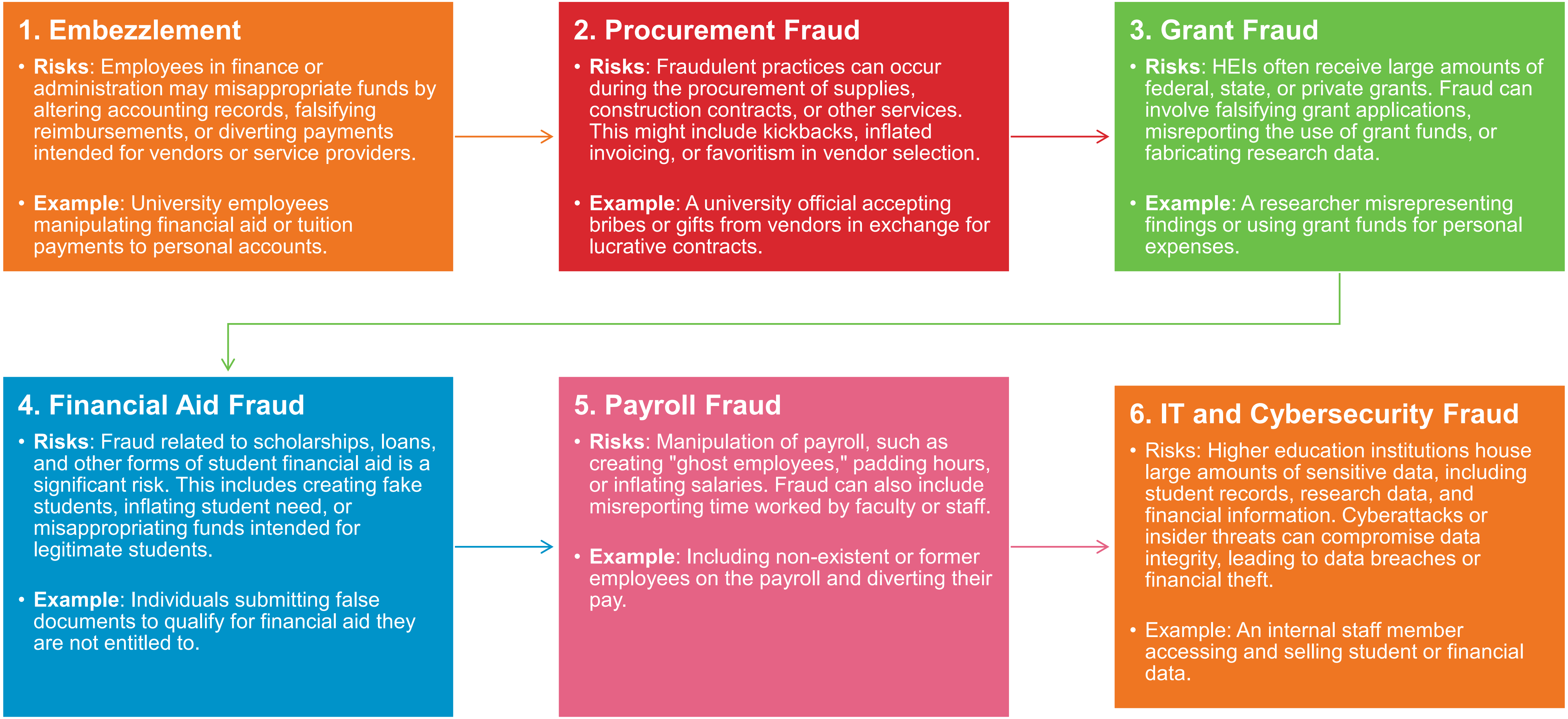
- Many higher education faculty members are unaware of cybersecurity threats and don't know how to respond to them.

FRAUD RISKS

RELATED TO HIGHER EDUCATION



Higher Education Institutions (HEI) Fraud Risks



1. Embezzlement

- **Risks**: Employees in finance or administration may misappropriate funds by altering accounting records, falsifying reimbursements, or diverting payments intended for vendors or service providers.
- **Example**: University employees manipulating financial aid or tuition payments to personal accounts.

2. Procurement Fraud

- **Risks**: Fraudulent practices can occur during the procurement of supplies, construction contracts, or other services. This might include kickbacks, inflated invoicing, or favoritism in vendor selection.
- **Example**: A university official accepting bribes or gifts from vendors in exchange for lucrative contracts.

3. Grant Fraud

- **Risks**: HEIs often receive large amounts of federal, state, or private grants. Fraud can involve falsifying grant applications, misreporting the use of grant funds, or fabricating research data.
- **Example**: A researcher misrepresenting findings or using grant funds for personal expenses.

4. Financial Aid Fraud

- **Risks**: Fraud related to scholarships, loans, and other forms of student financial aid is a significant risk. This includes creating fake students, inflating student need, or misappropriating funds intended for legitimate students.
- **Example**: Individuals submitting false documents to qualify for financial aid they are not entitled to.

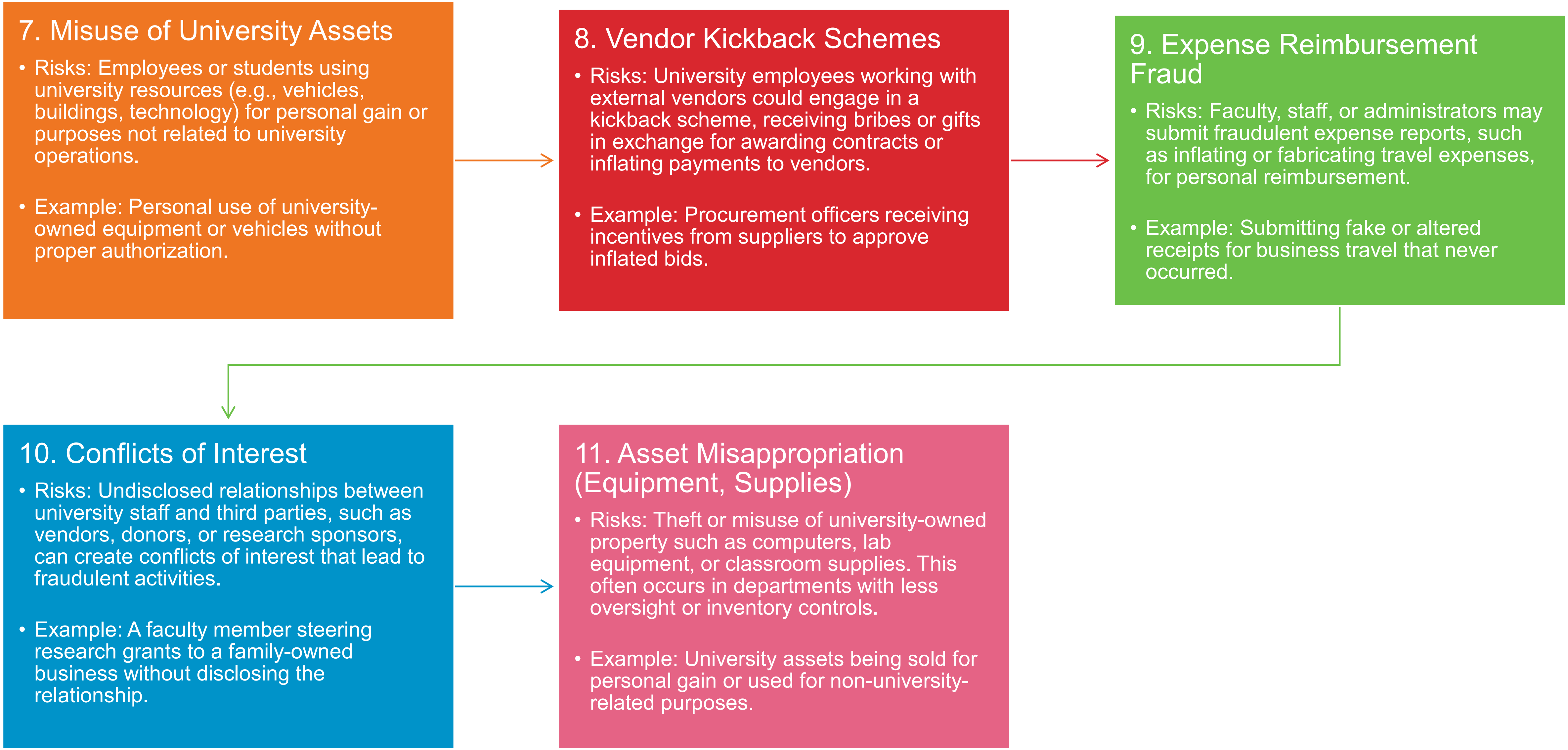
5. Payroll Fraud

- **Risks**: Manipulation of payroll, such as creating "ghost employees," padding hours, or inflating salaries. Fraud can also include misreporting time worked by faculty or staff.
- **Example**: Including non-existent or former employees on the payroll and diverting their pay.

6. IT and Cybersecurity Fraud

- Risks: Higher education institutions house large amounts of sensitive data, including student records, research data, and financial information. Cyberattacks or insider threats can compromise data integrity, leading to data breaches or financial theft.
- Example: An internal staff member accessing and selling student or financial data.

Higher Education Institutions (HEI) Fraud Risks cont.



7. Misuse of University Assets

- Risks: Employees or students using university resources (e.g., vehicles, buildings, technology) for personal gain or purposes not related to university operations.
- Example: Personal use of university-owned equipment or vehicles without proper authorization.

8. Vendor Kickback Schemes

- Risks: University employees working with external vendors could engage in a kickback scheme, receiving bribes or gifts in exchange for awarding contracts or inflating payments to vendors.
- Example: Procurement officers receiving incentives from suppliers to approve inflated bids.

9. Expense Reimbursement Fraud

- Risks: Faculty, staff, or administrators may submit fraudulent expense reports, such as inflating or fabricating travel expenses, for personal reimbursement.
- Example: Submitting fake or altered receipts for business travel that never occurred.

10. Conflicts of Interest

- Risks: Undisclosed relationships between university staff and third parties, such as vendors, donors, or research sponsors, can create conflicts of interest that lead to fraudulent activities.
- Example: A faculty member steering research grants to a family-owned business without disclosing the relationship.

11. Asset Misappropriation (Equipment, Supplies)

- Risks: Theft or misuse of university-owned property such as computers, lab equipment, or classroom supplies. This often occurs in departments with less oversight or inventory controls.
- Example: University assets being sold for personal gain or used for non-university-related purposes.

How Can Fraud 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

- **Morale Issues -** Fraud can harm morale among employees

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.

- Living beyond means 39%
- Financial difficulties 27%
- Unusually close association with vendor/customer 20%
- No behavioral red flags 16%
- Control issues, unwillingness to share duties 13%
- “Wheeler-dealer” attitude 12%
- Irritability, suspiciousness, or defensiveness 12%
- Bullying or intimidation 11%
- Divorce/family problems 10%

Occupational Fraud: A Report to the Nations 2024

Higher Education Fraud cases

POLL QUESTION #3

HAVE YOU EVER ENCOUNTERED A GHOST STUDENT???

1. YES
2. NO
3. I DON'T KNOW
4. SHOULD I CALL GHOSTBUSTERS?

Ghost Students, and How They Operate

- Ghost students, as their name implies, aren't real people. They are aliases or stolen identities used by scammers and the bots they deploy to get accepted to a college, but not for the purpose of attending classes or earning a degree.

- A ghost student is created when a fraudster completes an online application to a college or university and then, once accepted, enrolls in classes. At that point, the fraudster behind the ghost student can use the fake identity to act like a regular student. He or she can access, and abuse cloud storage provided by the institution or use a college-provided VPN or .edu email address to perpetrate other scams. In the most serious cases, a ghost student's new enrollment status may be used to apply for and receive thousands of dollars in financial aid.

- It's become easier to pull off this fraud since the start of the COVID-19 pandemic and the transition to online learning because students no longer have to appear in person on campus to enroll. Community colleges are particularly at risk for ghost students because of their simpler application processes, lower admission standards and preponderance of online course offerings.

- In one case brought by the U.S. Department of Justice in March 2023, three women were accused of running a ghost student scam that used the identities of prison inmates and others to enroll in a California community college. They allegedly received nearly $1 million in federal student loans.

- For institutions subject to these scams, the consequences can range from annoying to expensive. Ghost students can disrupt operations on campus by taking spots from actual qualified students who have applied or by forcing institutions to add sections for courses with high interest, only to see those seats sit empty.

https://edtechmagazine.com/higher/what-are-ghost-students-perfcon

Former Assistant Dean and Two Other Former Employees of Essex County Graduate School Admit Million-Dollar Embezzlement

NEWARK, N.J. – A former assistant dean and two other former employees of an Essex County graduate school pled guilty to defrauding their former employer of more than $1.3 million, U.S. Attorney Philip R. Sellinger announced.

Pled guilty to wire fraud conspiracy:

- Teresina DeAlmeida, 59, of Warren, New Jersey
- Rose Martins, 44, of East Hanover, New Jersey
- Silvia Cardoso, 61, of Warren, New Jersey

According to documents filed in this case and statements made in court:

Between 2009 and July 2022, DeAlmeida, Martins, and Cardoso conspired to fraudulently misappropriate more than $1.3 million from their former employer, a graduate school of a university in Essex County, New Jersey.

DeAlmeida was an assistant dean responsible for financial functions, and Martins served as her assistant. Cardoso, DeAlmeida's sister, was also employed by the graduate school in a support staff role.

The defendants used a variety of methods to defraud the university:

*Beginning in 2009, DeAlmeida directed a graduate school vendor to pay Martins and Cardoso as though they worked for the vendor. DeAlmeida and Martins then caused the vendor to submit false invoices to the graduate school over the course of approximately four years..

*From 2010 through 2022, DeAlmeida and Martins directed graduate school vendors to order hundreds of thousands of dollars of gift cards and prepaid debit cards the conspirators used for their personal benefit.

Then to submit fraudulent invoices to the school purporting to be for goods and services that were never provided.

The conspirators also misused DeAlmeida's school-issued credit card to purchase hundreds of thousands of dollars of gift cards and prepaid debit cards from the school's bookstore.

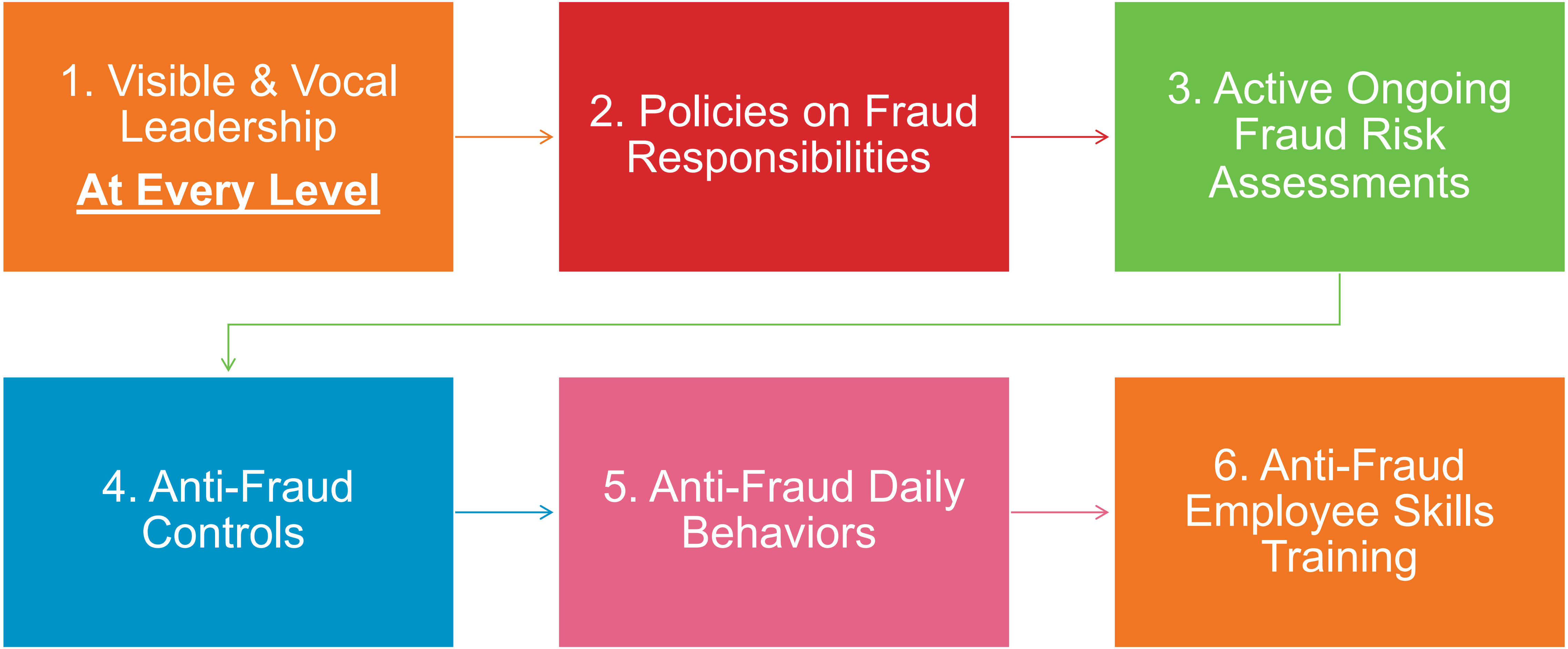
*In 2015, Martins opened a shell entity called CMS Content Management Specialist LLC. Martins submitted, and DeAlmeida approved, fraudulent invoices totaling more than $208,000.

*The conspirators also used DeAlmeida's school-issued credit card to make tens of thousands of dollars in unauthorized personal purchases. More than $70,000 in purchases at an online retailer shipped directly to their homes, including woman's shoes, smart watches, and bed linens. DeAlmeida and Martins fraudulently altered certain receipts before submitting them to the school for payment.

https://www.justice.gov/usao-nj/pr/former-assistant-dean-and-two-other-former-employees-essex-county-graduate-school-admit

Preventing and Mitigating Fraud

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

HCC Policies on Fraud Responsibilities

BBFB (LEGAL)

CAK (LEGAL)

CDC (LOCAL)

CDE (LOCAL)

DGBA (LOCAL)

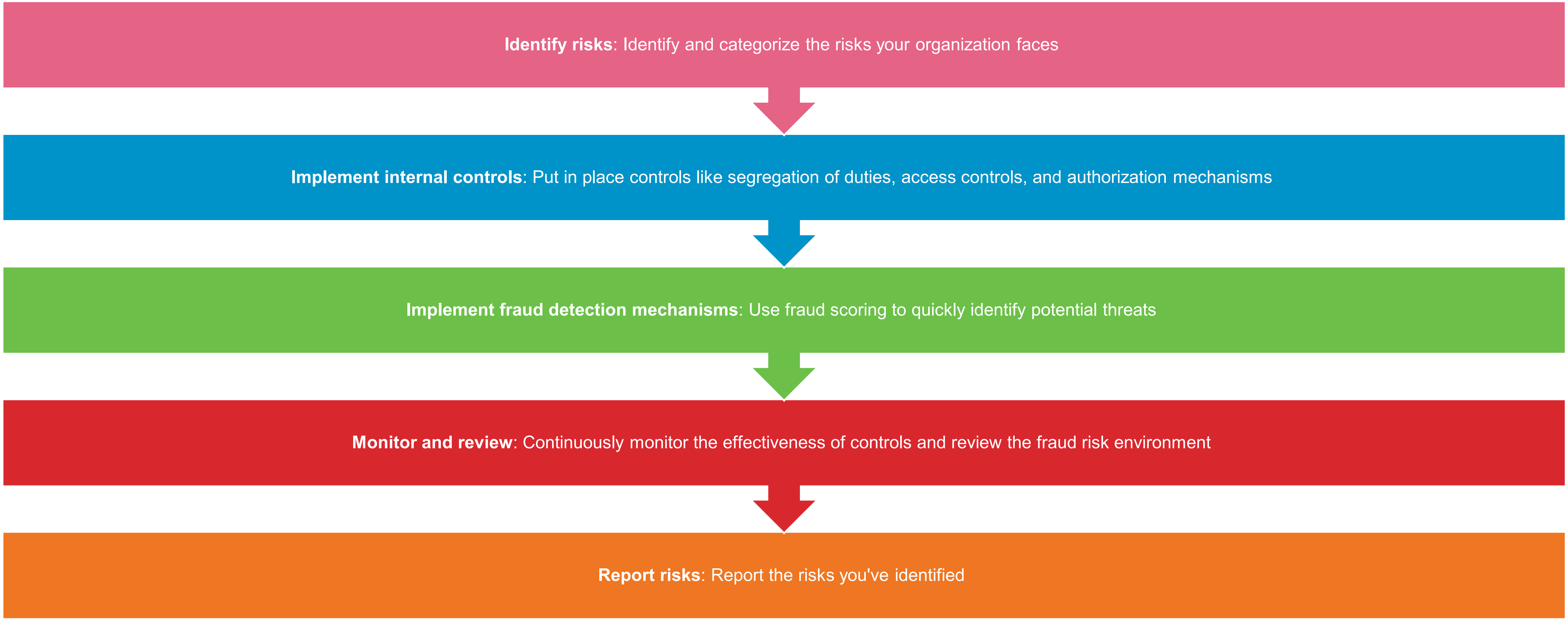
DH (LOCAL)

FEA (LOCAL)

FLB (LOCAL)

FLD (LOCAL)

Conducting a Fraud Risk Assessment



Identify risks: Identify and categorize the risks your organization faces

Implement internal controls: Put in place controls like segregation of duties, access controls, and authorization mechanisms

Implement fraud detection mechanisms: Use fraud scoring to quickly identify potential threats

Monitor and review: Continuously monitor the effectiveness of controls and review the fraud risk environment

Report risks: Report the risks you've identified

Regularly updating and reviewing your risk assessments can help you stay ahead of potential fraudsters.

Anti-Fraud Controls

Primary weakness contributing to fraud – LACK OF CONTROLS

Trust is not a control!

https://www.recharged-education.com/pcardblog/2020/8/6/trust-is-not-a-control

INTERNAL CONTROLS

Internal controls are a company's rules, procedures, and mechanisms that help ensure the accuracy of financial information, prevent fraud, and promote accountability.

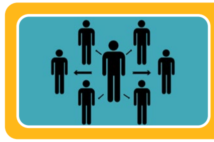
When properly designed and executed, will help ensure your area has optimal safeguards against loss, errors, or fraud.

A good internal control system includes both preventive and detective controls.

TYPES OF CONTROLS

Preventive Controls

Aim to decrease the chance of errors and fraud before they occur.


Separation of duties

Pre-approval of actions and transactions (such as a Travel Authorization)

Access controls (such as passwords)

Physical control over assets (i.e. locks on doors or a safe for cash/checks)

Employee screening and training

Detective Controls

Designed to find errors or problems after the transaction has occurred.

Monthly reconciliations of departmental transactions

Review organizational performance (such as a budget-to-actual comparison to look for any unexpected differences)

Physical inventories (such as a cash or inventory count)

Anti-Fraud Employee Skills Training

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

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

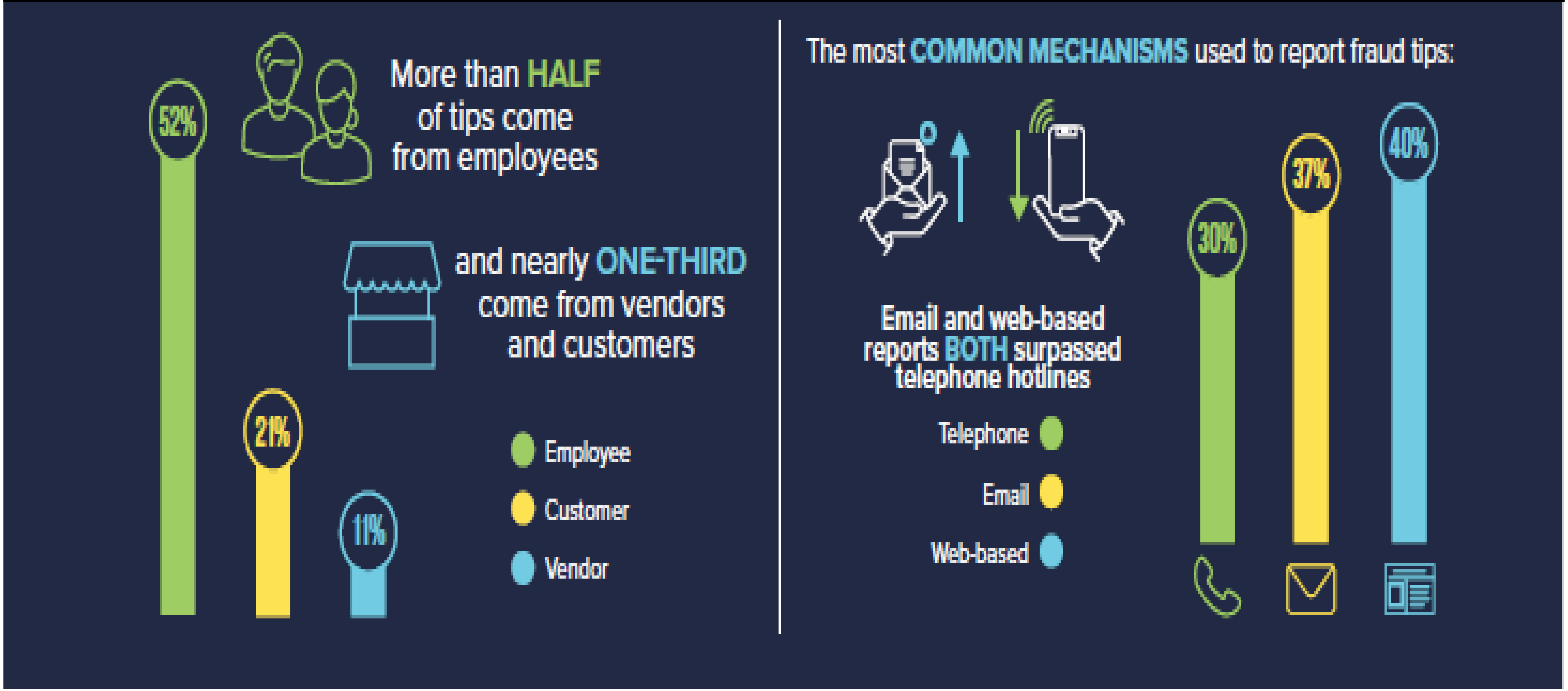
POLL QUESTION #4

WHO IS RESPONSIBLE FOR REPORTING POSSIBLE FRAUDULENT ACTIVITY?

A. Supervisor
B. HCC Police
C. Staff
D. Everyone

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

INITIAL DETECTION OF OCCUPATIONAL FRAUD



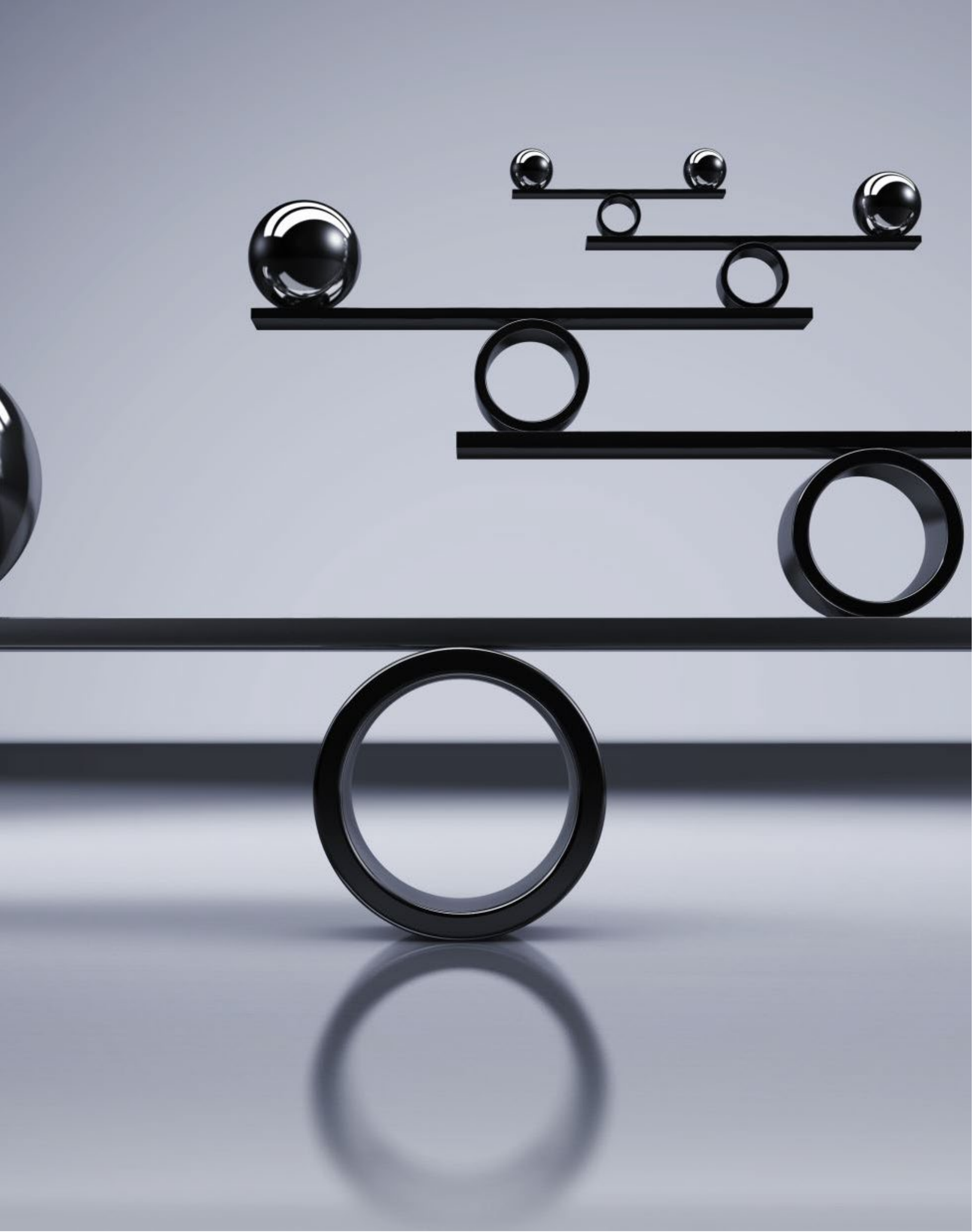
More than **HALF** of tips come from employees

and nearly **ONE-THIRD** come from vendors and customers

The most **COMMON MECHANISMS** used to report fraud tips:

Email and web-based reports **BOTH** surpassed telephone hotlines

Encourage a culture of ethics and transparency!



Ethics –Two Categories

Personal

- Individual’s basic notion of right and wrong

Organizational

- Consciously defined by organizations to promote consistent integrity in the members

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!!

- 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

Why People Don’t Speak Up

HCC partners with an external provider, **EthicsPoint**, to provide the Ethics and Compliance Hotline (the “Hotline”) for employees, students, and members of the public to report alleged:

1. Noncompliance with laws;
2. Noncompliance with College District policies, regulations, or Codes of Conduct; and
3. **Occupational fraud, waste, or abuse of authority, resources, or taxpayer dollars.**

http://www.hccs.ethicspoint.com

1.855.811.6284

The Hotline is available 24 hours a day, 7 days a week.

Other Common Fraud Schemes on the rise…

Business Email Compromise

Business email compromise (BEC) is one of the most financially damaging online crimes. It exploits the fact that so most of us rely on email to conduct both our personal and professional business.

In a BEC scam—also known as email account compromise (EAC)—criminals send an email message that appears to come from a known source making a legitimate request, like in these examples:

- A vendor your company regularly deals with sends an invoice with an updated mailing address.
- A company CEO asks her assistant to purchase dozens of gift cards to send out as employee rewards. She asks for the serial numbers so she can email them out right away.
- A homebuyer receives a message from his title company with instructions on how to wire his down payment.

How BEC Scams Work

A scammer might:

- Spoof an email account or website. Slight variations on legitimate addresses (john.kelly@examplecompany.com vs. john.kelley@examplecompany.com) fool victims into thinking fake accounts are authentic.
- Send spearphishing emails. These messages look like they're from a trusted sender to trick victims into revealing confidential information. That information lets criminals access company accounts, calendars, and data that gives them the details they need to carry out the BEC schemes.
- Use malware. Malicious software can infiltrate company networks and gain access to legitimate email threads about billing and invoices. That information is used to time requests or send messages, so accountants or financial officers don't question payment requests. Malware also lets criminals gain undetected access to a victim's data, including passwords and financial account information.

https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise

Elder Fraud

Each year, millions of elderly Americans fall victim to some type of financial fraud or confidence scheme, including romance, lottery, and sweepstakes scams—just to name a few.

Seniors are often targeted because they tend to be trusting and polite. They also usually have financial savings, own a home, and have good credit—all of which make them attractive to scammers.

Additionally, seniors may be less inclined to report fraud because they don't know how, or they may be too ashamed at having been scammed.

They might also be concerned that their relatives will lose confidence in their abilities to manage their own financial affairs. And when an elderly victim does report a crime, they may be unable to supply detailed information to investigators.

With the elderly population growing and seniors racking up more than $3 billion in losses annually, elder fraud has remained a growing problem.

Common Elder Fraud Schemes

Scammers targeting elder citizens may employ one or more of the following types of schemes:

- Romance scam: Criminals pose as interested romantic partners on social media or dating websites to capitalize on their elderly victims' desire to find companions.

- Tech support scam: Criminals pose as technology support representatives and offer to fix non-existent computer issues. The scammers gain remote access to victims' devices and sensitive information.

Grandparent scam: A type of confidence scam where criminals pose as a relative—usually a child or grandchild—claiming to be in immediate financial need.

https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/elder-fraud

SEXTORTION

The FBI has seen a huge increase in the number of cases involving children and teens being threatened and coerced into sending explicit images online—a crime called sextortion.

Sextortion can start on any site, app, messaging platform, or game where people meet and communicate.

In some cases, the first contact from the criminal will be a threat. The person may claim to already have a revealing picture or video of a child that will be shared if the victim does not send more pictures.

More often, however, this crime starts when young people believe they are communicating with someone their own age who is interested in a relationship or with someone who is offering something of value.

FINANCIAL SEXTORTION is different than traditional sextortion.

In these cases, the offender receives sexually explicit material from the child and then threatens to release the compromising material unless the victim sends money and/or gift cards. The amount requested varies, and the offender often releases the victim's sexually explicit material regardless of whether or not they receive payment. **This increasing threat has resulted in an alarming number of deaths by suicide.**

Ransomware

Ransomware is a type of malicious software—or malware—that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return.

Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.

You can unknowingly download ransomware onto a computer by opening an email attachment, clicking an ad, following a link, or even visiting a website that's embedded with malware.

Ransomware Incident

In February, Change Healthcare, a subsidiary of UnitedHealth, was hit by a devastating ransomware attack from the notorious BlackCat gang. Using stolen credentials, the attackers gained access to Change's data systems, exfiltrating up to 4TB of sensitive patient data. They then deployed ransomware that crippled healthcare billing, payment operations and other critical processes. This breach has been labeled as one of the most consequential attacks ever to strike the U.S. healthcare system.

https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware

HCC | HOUSTON COMMUNITY COLLEGE
INTERNAL AUDIT DEPARTMENT

See
Something
Say
Something

Terry Corrigan, Internal Audit Director

713-718-7278

hcc.internalaudit@hccs.edu

https://www.hccs.edu/departments/internal-auditing/

Thank you!