ACFE
Association of Certified Fraud Examiners

Together, Reducing Fraud Worldwide

External Fraud Targeting Government Agencies

Jason Zirkle, CFE, CAMS

Training Director, Association of Certified Fraud Examiners

(Previously with the Texas Department of Public Safety)

© 2019 Association of Certified Fraud Examiners, Inc.

Increase in COVID-19 Fraud Schemes

- Government auditors already have a ton to worry about!
  - Corruption
  - Cyber threats
  - Procurement / Vendor Fraud
  - Business email compromise scams
  - Embezzlement
  - Healthcare & Insurance fraud
- The COVID-19 pandemic has added to the misery
  - A significant increase in external fraud risks
  - More employees working remotely, adding new cyber threats & making fraud investigations more difficult
  - A massive increase in public funds being issued to citizens, creating an attractive target for serial fraudsters

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Increase in COVID-19 Fraud Schemes

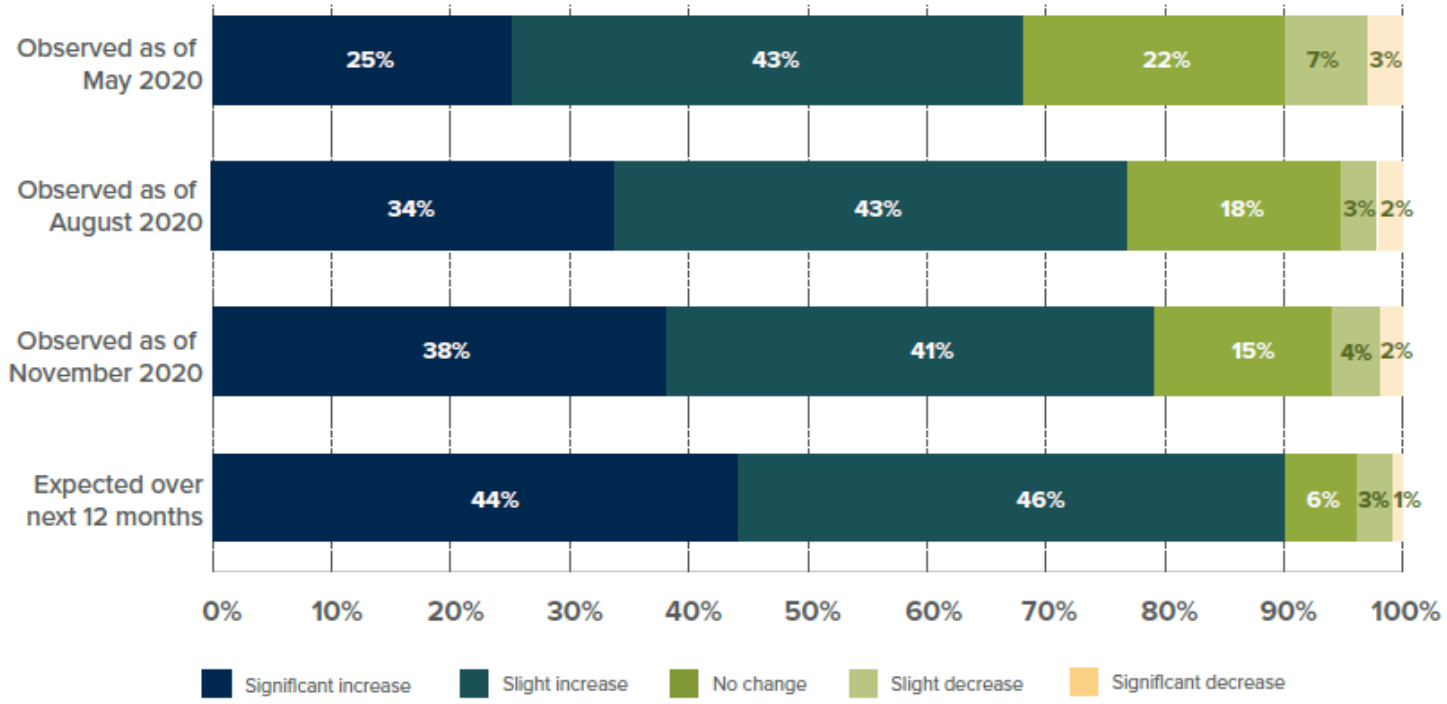
The ACFE has many resources to help you:

- Educate organizational leadership and staff, as well as the general public, about the effects of the pandemic on the fight against fraud
- Update or undertake formal fraud risk assessments to understand and reflect the new fraud risk landscape
- Build support for continued investment in anti-fraud programs
- Navigate the challenges of preventing, detecting, and investigating fraud in the current environment

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

ACFE Fraud in the Wake of COVID-19: Benchmarking Report

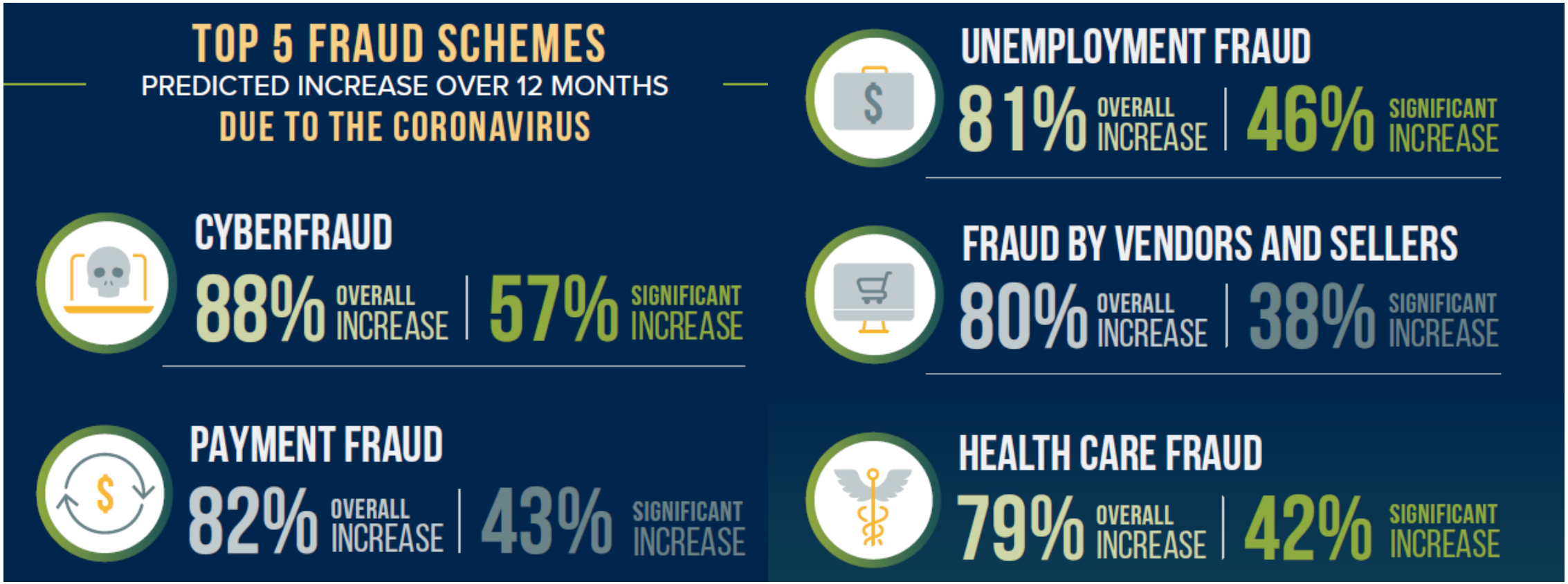
FIG. 1 Change in the overall level of fraud



- In May 2020, 68% of ACFE members reported an overall increase in fraud
- In Nov. 2020, this increased to 79%
- 90% of respondents expected an increase over the next 12 months

© 2019 Association of Certified Fraud Examiners, Inc.

Top 5 Fraud Schemes



© 2019 Association of Certified Fraud Examiners, Inc.

Serial Fraudsters & COVID-19

- Serial fraudsters think differently than the rest of us. They do nothing but sit around and come up with new ways to defraud people
- Natural disasters such as the COVID-19 pandemic are a *perfect* time to strike:
  - Consumers are vulnerable – During a disaster, fraud is the last thing on their minds. They may want products to keep themselves safe, and they want constant news related to the disaster.
  - Governments, law enforcement, regulators are temporarily focused more on the disaster than they are on fraud.
- Brett Johnson & podcast

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Cybercrime & Cyberfraud

© 2019 Association of Certified Fraud Examiners, Inc.

Cybercrime / Cyberfraud

- According to our members, cybercrime & cyberfraud have seen the highest increase of all fraud schemes in the wake of COVID-19
- 88% of our members report seeing an increase in cybercrime, with 57% seeing a “significant” increase
- Government agencies have always been a target for cybercriminals:
  - Tend to have smaller budgets for cybersecurity than the private sector
  - Tend to have lots of information attractive to criminals (Individual & company PII, bank accounts, confidential data, etc)

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Cybercrime & Cyberfraud

- Interpol reports a massive increase in the following schemes:
  - Online scams & phishing
  - Disruptive malware
  - Data harvesting malware
  - Malicious domains
  - Social engineering
  - Business email compromise schemes

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Phishing & Malware – Key terms

- ***Malware*** is any malicious software used to damage devices, steal data, or gain unauthorized access.
- ***Phishing*** is any fraudulent communication that purports to be from a legitimate sender to induce a victim to reveal financial data, email credentials, etc.
- ***SMiShing*** is similar to phishing but uses SMS text messages instead of email.
- ***Spoofing*** occurs when a communication from an unknown source (often criminal) is disguised as a known, legitimate source.

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Types of Malware

Type	What It Does
Ransomware	Disables victim's access to data until ransom is paid
Fileless Malware	Makes changes to files that are native to the OS
Spyware	Collects user activity data without their knowledge
Adware	Serves unwanted advertisements
Trojans	Disguises themselves as desirable code
Worms	Spread through a network by replicating themselves
Rootkits	Gives hackers remote control of a victim's device
Keyloggers	Monitors users' keystrokes
Bots	Launches a broad flood of attacks
Mobile Malware	Infects mobile devices

ACFE
Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Phishing and Malware Key Players

- Major players in phishing and malware:
  - ***Programmers*** write code and create malware packs that they sell in dark web marketplaces. They typically make money by creating and selling the malware and not to commit cyberfraud.
  - ***Cyberfraudsters*** are typically not trained hackers. They purchase "off-the-shelf" malware packages on the dark web, and they use these to commit cyberfraud.
  - ***Cashiers and tellers*** are a network of criminals who assist fraudsters in converting stolen data into cash and helping them launder the funds (for a fee).

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Other Cybercrime Issues

- Business email compromise scams
  - Review current policies
  - Employee training
  - Separation of duties
  - Management override of internal controls
- Cybercrime targeting the COVID-19 vaccine pipeline
- Working with your IT department

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Cybercrime Internal Controls

- Should be a blend of technical & administrative controls:
- Technical
  - Logical access controls (process where users are identified & given access)
  - Network security (firewalls, intrusion detection, etc)
  - Encryption
  - Application security
- Administrative
  - Security policies & awareness training
  - Separation of duties
  - Computer risk assessments, audits, etc
  - Incident response plans

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Unemployment Fraud

© 2019 Association of Certified Fraud Examiners, Inc.

Unemployment Fraud

- Prior to COVID, US Dept. of Labor estimated improper payments accounted for 10.61% of $31 billion in unemployment benefits
- Then, a record 36.5 million applied for unemployment in 2 months, overwhelming state agencies, many of which waived certification and work search requirements for quicker payments

For months, fraudsters have exploited programs designed to swiftly distribute federal pandemic aid to self-employed and contract workers. | David McNew/Getty Images

California inmates part of $1B unemployment fraud schemes, prosecutors say

By **KATY MURPHY** | 11/24/2020 02:35 PM EST | Updated 11/24/2020 07:40 PM EST

Share on Facebook Share on Twitter

Sophisticated crime rings involving inmates in California's jails and prisons may have stolen upwards of $1 billion in pandemic unemployment aid, four district attorneys and a federal

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Unemployment Fraud

1. Fraudulent first-time claims: *Fraudster uses stolen PII to file a claim. Can be a one-off, or can be in bulk*
   - If feasible, consider batch or individual lookup capabilities against public records (vital stats, state incarceration data, etc) and 3rd party data programs
   - Invest in the ability to search for duplicate attributes (shared addresses, emails phone numbers, IP addresses, etc)
2. Fictitious business scams: *Fraudsters use two-sided tactics to file claim. Stolen PII used for the claimant, stolen or fake PII for employer*
   - Cross-check employers associated with claims against lists of businesses that have opened or reactivated since the start of the pandemic

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Unemployment Fraud

3. Benefit-wage conflicts: *"Second wave" of fraud, claimant returns to work, but fails to notify state agency and continues to be paid*
   - Program integrity departments traditionally view this as a minor loss, but it could grow significantly with the pandemic
   - Make sure you have the ability to identify claimants who return to work as quickly as possiblee

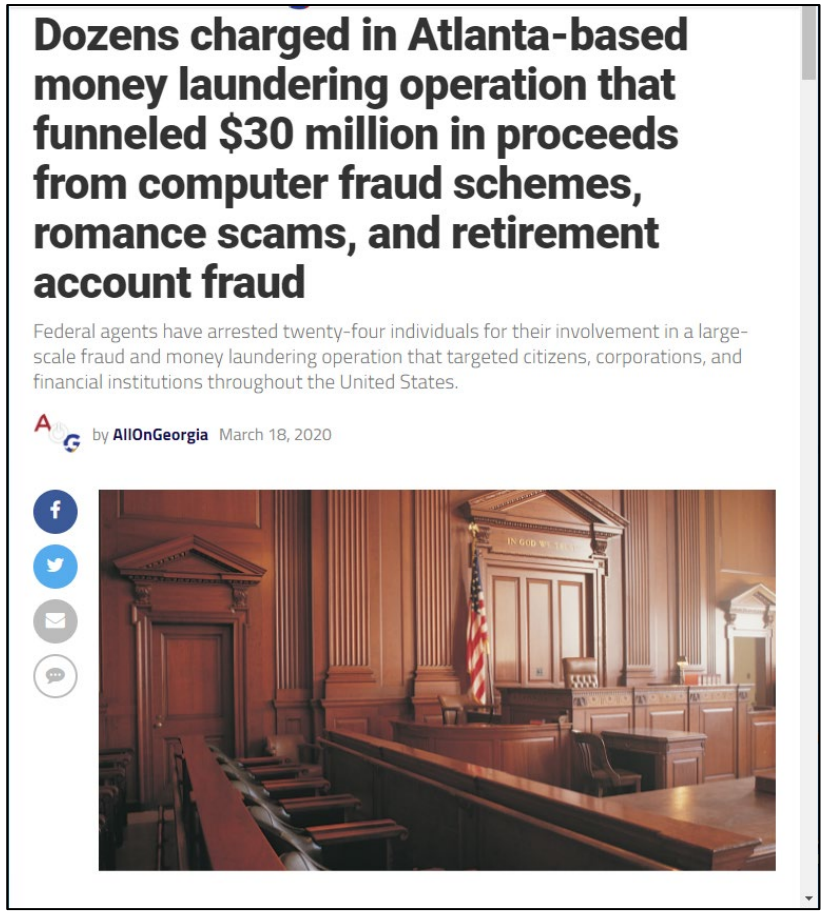
ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Account Takeovers

© 2019 Association of Certified Fraud Examiners, Inc.

Account Takeovers

- Account takeovers were already increasing prior to the pandemic!
  1. Account is compromised
  2. Banking account info is changed
  3. Payments routed elsewhere, often to prepaid card account controlled by a “catcher” or a “money mule”
  4. Funds are eventually transferred to the main fraudsters, often overseas
  5. Funds may go to purchase used vehicles or some other commodity which is shipped overseas
  6. Victims have almost no chance of recovering their funds



Dozens charged in Atlanta-based money laundering operation that funneled $30 million in proceeds from computer fraud schemes, romance scams, and retirement account fraud

Federal agents have arrested twenty-four individuals for their involvement in a large-scale fraud and money laundering operation that targeted citizens, corporations, and financial institutions throughout the United States.

by AllOnGeorgia March 18, 2020

© 2019 Association of Certified Fraud Examiners, Inc.

Account Takeovers

- Employee direct deposit phishing: Common with employers that use self-service direct-deposit platforms
- Similar to business email compromise, fraudster impersonates employer via email with the goal of getting the victim to reveal login credentials, which are used to access PII and/or redirect deposits
  - Alert employees & train them on phishing
  - Implement two-step or multi-factor verification for HR/payroll platforms
  - Require IT to monitor unusual activity (such as large number of accounts having contact & bank info changed over short period)
  - Policy of temporarily reverting to paper check after banking change

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Account Takeovers

- Government pension plan account takeovers: Fraudsters target elderly & retirees through a variety of ways
  - Alert retirees/members to monitor accounts
  - Programs must have multiple points of identity verification using traditional and nontraditional data
  - Require IT to monitor unusual activity (such as large number of accounts having contact & bank info changed over short period)
  - Log IP addresses!
  - Policy of temporarily reverting to paper check after banking change
  - Consider restricting payments to prepaid card accounts

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Account Takeovers

- Corporate account takeovers: Phishing, BEC, malware, social engineering can be used to access corporate bank account credentials
  - Take fresh look at risk assessments with an eye on emerging trends & tactics used by hackers
  - Employee training on understanding of risks
  - Managing corporate account users
  - Have an account takeover incident response plan in place
  - Work with bank to minimize ways to access funds if accounts are taken over (Wire blocks or filters, ACH blocks or filters, positive pay, etc)

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Vendor / Procurement Fraud

© 2019 Association of Certified Fraud Examiners, Inc.

Vendor / Procurement Fraud

- Schemes involving collusion among vendors:
- Complementary bidding
  - Competitors submit token bids that are not serious attempts to win the contract.
  - Token bids give the appearance of genuine bidding, but, by submitting token bids, the conspirators can influence the contract price and who is awarded the contract.

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Monday, December 21, 2020

Government Contractor Admits Scheme to Inflate Costs on Federal Projects and Pays $11 Million to Resolve Criminal and Civil Probes

Schneider Electric Buildings Americas Inc. (Schneider Electric), a nationwide provider of electricity solutions for buildings and data centers with its principal place of business in Carrollton, Texas, will pay $11 million to resolve criminal and civil investigations relating to kickbacks and overcharges on eight federally-funded energy savings performance contracts (ESPCs), the Department of Justice announced today. Under the contracts, Schneider Electric was to install a variety of energy savings upgrades, such as solar panels, LED lighting, and insulation, in federal buildings.

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Vendor / Procurement Fraud

- Bid rotation
  - Two or more contractors conspire to alternate the business among themselves on a rotating basis.
- Bid suppression
  - Two or more contractors enter into an illegal agreement whereby at least one of the conspirators refrains from bidding or withdraws a previously submitted bid to ensure that a particular competitor's bid is accepted.
- Market division
  - Competitors agree to divide and allocate markets and to refrain from competing in each other's designated portion of the market.

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Vendor / Procurement Fraud

- Schemes Involving Collusion Between Contractors and Employees
- Need recognition
  - Procurement employees convince their employer that it needs excessive or unnecessary products or services
  - Often, purchasing entity employees receive a bribe or kickback for convincing their employer to recognize a need for a particular product or service
- Bid tailoring
  - An employee with procurement responsibilities, often in collusion with a contractor, drafts bid specifications in a way that gives an unfair advantage certain contractor
- Bid manipulation
  - A procuring employee manipulates the bidding process to benefit a favored contractor or supplier

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Vendor / Procurement Fraud

- Prevention and Detection:
  - Monitoring procurement activities: Agencies should implement a continuous, self-auditing program to monitor the performance of their procurement activities
  - Vendor management: Management should take steps to prevent and detect criminal conduct by its vendors, such as:
    - Vendor background checks
    - Controls for vendor master file management
    - Vendor monitoring (focus on red flags & fraud risk)
- Public school system case study

ACFE Association of Certified Fraud Examiners
© 2019 Association of Certified Fraud Examiners, Inc.

Questions?

Jason Zirkle, CFE

Training Director, ACFE

Phone: 512-478-9000 x113

E-mail: JZirkle@acfe.com

© 2019 Association of Certified Fraud Examiners, Inc.