Clark County Annual Fraud Seminar

December 17, 2020

Lindsay Osborne
Program Manager

Cheryl Friesen
County Subject Matter Expert

Sherrie Ard, CPA, CFE
Center for Government Innovation Program Manager

Office of the
Washington
State Auditor
Pat McCarthy

Session overview

- Audits in a virtual environment
- Risks related to county audits
- Resources available to help

Audits in a virtual environment

- How audits look now?
  - ✓ Audits are being performed remotely

- Communication and coordination
  - ✓ Document requests
  - ✓ How to share records
  - ✓ Timing

Issue by Category for Counties

Area of Issue	ML	Finding
Federal procurement - Highway Planning	5	2
Financial statement preperation	3	3
Cash receipting	1	
ER&R billing rates	1	
Self-insurance	1	
Restricted funds - Building and Planning	2	
Procurement - purchases and public works	1	1
Purchase card use	1	
Gift card purchases	1	
Suspension and debarment -federal single audits		3
Use of resticted funds - REET	2	
Davis-Bacon Act (prevailing wage rate) - federal single audits		1
Financial Condition		1
Reporting - federal single audits		1
Rural counties sales and use tax	3	1
Use of resticted funds - lodging tax		1
County Road Fund	1	

Audit Issues

We will focus on the following Issues:
- Federal Procurement
- Federal Suspension and Debarment
- Restricted Funds – Building and Planning
- Restricted Funds - REET

Audit Issues

Federal Procurement
- The entity's procurement policy must specifically address what procurement procedures are followed when using federal funding and be the most restrictive of state, local and federal.
- The entity must have written standards of conduct that cover conflicts of interest

Audit Issues

We found issues with:
- No policy or procedures in place or too limited. Also missing thresholds from the procedures.
- Standards of Conduct Policy (conflict of interest) also missing in some cases

We also had a few issues with non-federal procurement. The Center has developed a bidding and buying guide resource to help with this area.
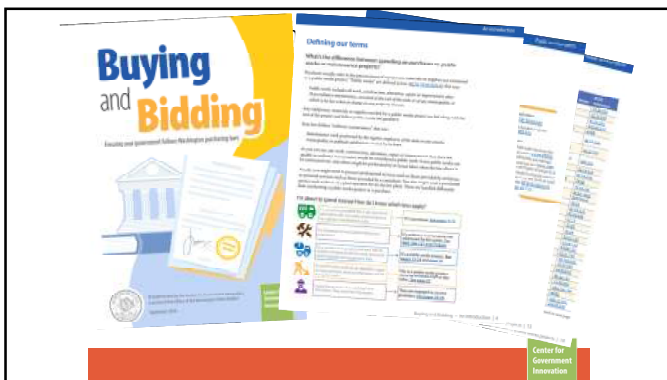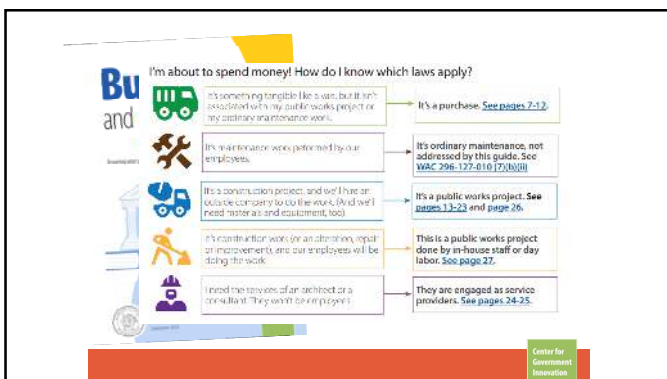
Resources to manage procurement

Is this Bidder Responsible?
Evaluation checklist for public contracts

Responsible Bidder Checklist

Office of the Washington State Auditor

Resources to manage procurement

Best Practices for Change Orders

Using Others' Bid Awards ('Piggybacking')

Office of the Washington State Auditor

Audit Issues

Federal Suspension and Debarment

- Required for all new contracts (purchases) over $25,000 and all new subrecipient contracts (no threshold)
- Verification can be a clause in contract, review the Excluded Parties List System (EPLS) or written certification from contractor

Audit Issues

We found Issues with:
- Not checking all contractors or sub contractors over $25,000 or not retaining evidence

Audit Issues

Restricted Funds - Building and Planning

Counties can collect permit fees to cover the following costs:
- Processing applications, inspecting and reviewing plans, and preparing detailed statements required by state environmental policy.

We found issues in a couple different Counties with:
- Not tracking the expense activity to demonstrate they were used for eligible costs

Audit Issues

Restricted Funds – Real Estate Excise Taxes (REET)
- State laws (RCW 82.46.010 and 82.46.035) restrict the use of these funds to finance capital projects specified in a capital facilities plan element of a comprehensive plan

We found issues with:
- The capital facilities plan not being adopted
- The capital facilities plan not including the approved REET projects as required by law
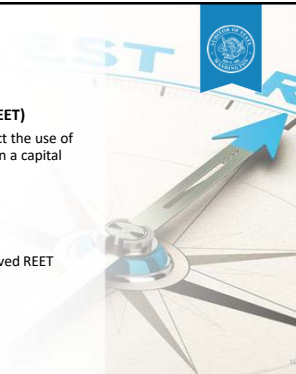
Required Risks To Assess

Electronic Funds Transfer (EFT) Controls
- We are testing controls on all audits due to increase in number of payroll and vendor EFT cyber related fraud
    - School District example
    - Direct deposit example

Required Risks To Assess

Restricted Funds
- There are several areas of risk our auditors consider in planning. There were two that we had multiple reportable issues on in fiscal year 2019 that I covered in the audit issues section.

Finding Center Resources

New COVID-19 Guidance Toolkit

Find the latest accounting, reporting and auditing resources here

Resources to manage internal controls

Resources to manage internal controls

Resources to manage internal controls

Resources to manage internal controls

#BeCyberSmart

#BeCyberSmart

#BeCyberSmart

Links to free training and resources

Nationally recognized sources
- Homeland Security
- MS-ISAC
- National Cybersecurity Alliance

#BeCyberSmart

Everyone plays a role in keeping your organization safe from cybersecurity attacks

Resources- #BeCyberSmart

Check out the blog

International Fraud Awareness Week is a great time to update your fraud fighting toolkit

NOVEMBER 16, 2020

This week, we will highlight resources and important information to help state and local governments update their fraud fighting toolkits. We encourage you to check out these resources and share them with your agency. ... CONTINUE READING →

SAO making our outgoing emails cyber-safer

NOVEMBER 12, 2020

The State Auditor's Office is changing some of the emails we send every week to better align with cybersecurity best practices. ... CONTINUE READING →

Options are available for moving to 'no contact' cash receipting

OCTOBER 29, 2020

The interactions between customer and cashier have become complicated by the pandemic. How do you collect payments but keep everyone safe? If you are capturing your actions, here are some resources that might help you ... CONTINUE READING →

Office of the
Washington
State Auditor
Pat McCarthy

Center for
Government
Innovation

Reduce your cyber risk while working from home

APRIL 22, 2020

As local government workers get accustomed to working from home, there are a couple things our information technology experts here at the State Auditor's Office want you to be aware of, especially in a few areas. This blog post covers the typical risk areas ... CONTINUE READING →

Changing your processes and controls? Remember these tips to minimize risk

APRIL 14, 2020

The coronavirus pandemic likely is forcing you to change how you do your work, such as processing payroll or paying your bills. We understand that local governments need to get the work done, but we'd like to help you manage the risks that can come with new processes. ... CONTINUE READING →

Protect confidential information while working at home

JUNE 3, 2020

As your employees continue to telework, they might be handling, transferring and storing confidential data at home differently than they did at their usual work location. Learn how to protect this information in this new work environment. ... CONTINUE READING →

Office of the
Washington
State Auditor
Pat McCarthy

Center for
Government
Innovation

Check out the blog

The Audit Connection Blog   Resources   Public Records   Contact SAO   Client Login

Office of the Washington State Auditor
Pat McCarthy

Search SAO   SEARCH

Reports & Data   Performance Audits   About Audits   Improving Government   BARS & Annual Filing   Report a Concern   About SAO

Check out the Audit Connection Blog!

Stay connected with us and don't miss out on the resources we publish covering topics like cybersecurity and government accounting, and upcoming training and events.

Read Audit Connection blog

Office of the Washington State Auditor Pat McCarthy

Sign up to be notified

Interested in assistance or resources from the Center?

Center@sao.wa.gov

Questions

Contact Information

Lindsay Osborne
lindsay.osborne@sao.wa.gov

Cheryl Friesen
cheryl.friesen@sao.wa.gov

Sherrie Ard
sherrie.ard@sao.wa.gov

Center Contact Information

Sherrie Ard, CPA, CFE
Program Manager
Center for Government Innovation
sherrie.ard@sao.wa.gov

Website: https://www.sao.wa.gov/

Contact for any questions about services
or resources
center@sao.wa.gov

Fraud Awareness Training

December 17, 2020

Arnold Pérez, Performance Auditor

Audit Services

What we will cover:
- Report to the Nations 2020 (ACFE)
- Fraud in the Wake of COVID-19: Benchmarking Report 2020 (ACFE)
- 6 Steps to Stop or Mitigate Insider Fraud Risks

Association of Fraud Examiners 2020 Report to the Nations

- What types of organizations are victimized by occupational fraud?

- What are the most common occupational fraud schemes in Government and public administration?

- What are the primary internal control weaknesses that contribute to occupational fraud?

- How Occupational Fraud is Concealed

- How is it detected and who reports it?

- Behavioral Red Flags of Fraud

- Fraud Training Works

What types of organizations are victimized by occupational fraud?

1. Private company 44%

2. Public company 26%

3. **Government 16%**

4. Nonprofit 9%

5. Other 5%

What levels of government are victimized by occupational fraud?

1. National 45%

2. **Local 32%**

3. State/provisional 21%

4. Other 2%
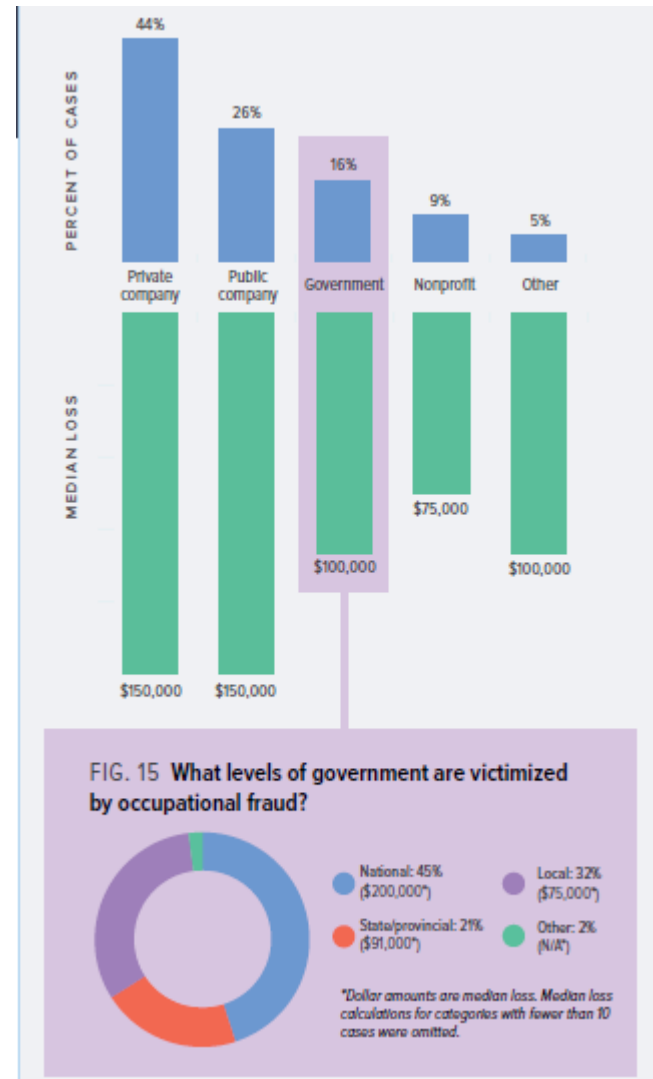
FIG. 15 **What levels of government are victimized by occupational fraud?**

National: 45% ($200,000*)
Local: 32% ($75,000*)
State/provincial: 21% ($91,000*)
Other: 2% (N/A*)

*Dollar amounts are median loss. Median loss calculations for categories with fewer than 10 cases were omitted.

What are the most common occupational fraud schemes in Government and public administration?

1. Corruption 48%
2. Billing 18%
3. Three-way tie 17%
   1. Expense reimbursement
   2. Noncash
   3. Payroll
4. Skimming 7%
5. Cash larceny 5%
6. Two-way tie 4%
   1. Check and payment tampering
   2. Financial statement fraud

Polling Question

- Which number of perpetrators creates the largest median loss?

  - One

  - Two

  - Three or More

Which number of perpetrators creates the largest median loss?

49% of cases
ONE PERPETRATOR
$90,000 Median loss

18% of cases
TWO PERPETRATORS
$105,000 Median loss

33% of cases
THREE OR MORE PERPETRATORS
$350,000 Median loss

What are the primary internal control weaknesses that contribute to occupational fraud?

32%-Lack of internal controls

18% -Lack of management review; Override of existing internal controls

10%-Poor tone at the top

6%-Lack of competent personnel in oversight roles; Other

5%-Lack of independent checks/audits

3%-Lack of employee fraud education

2%- Lack of clear lines of authority

<1% Lack of reporting mechanism
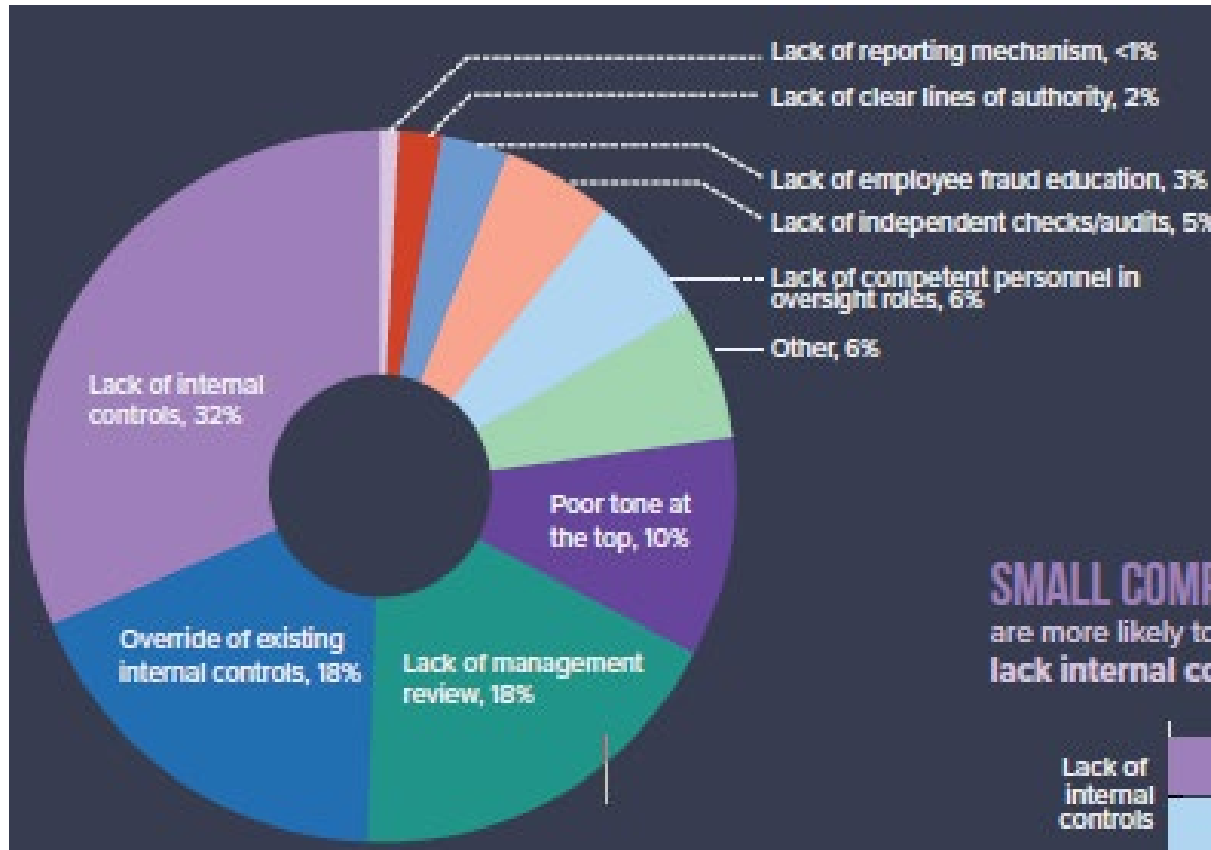
How Occupational Fraud is Concealed

TOP 4 CONCEALMENT METHODS USED BY FRAUDSTERS

40%
Created fraudulent physical documents

36%
Altered physical documents

27%
Altered electronic documents or files
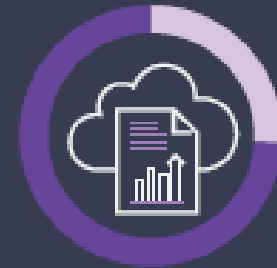
26%
Created fraudulent electronic documents or files
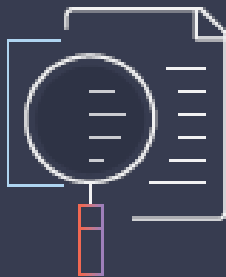
12% did not involve any attempts to conceal the fraud

How is it detected and who reports it?

Detection Method	Percentage
Tip	43%
Internal audit	15%
Management review	12%
Other	6%
By accident	5%
Account reconciliation	4%
External audit	4%
Document examination	3%
Surveillance/monitoring	3%
Notified by law enforcement	2%
IT controls	2%
Confession	1%

Who Reports	Percentage
Employee	50%
Customer	22%
Anonymous	15%
Vendor	11%
Other	6%
Competitor	2%
Shareholder/owner	2%
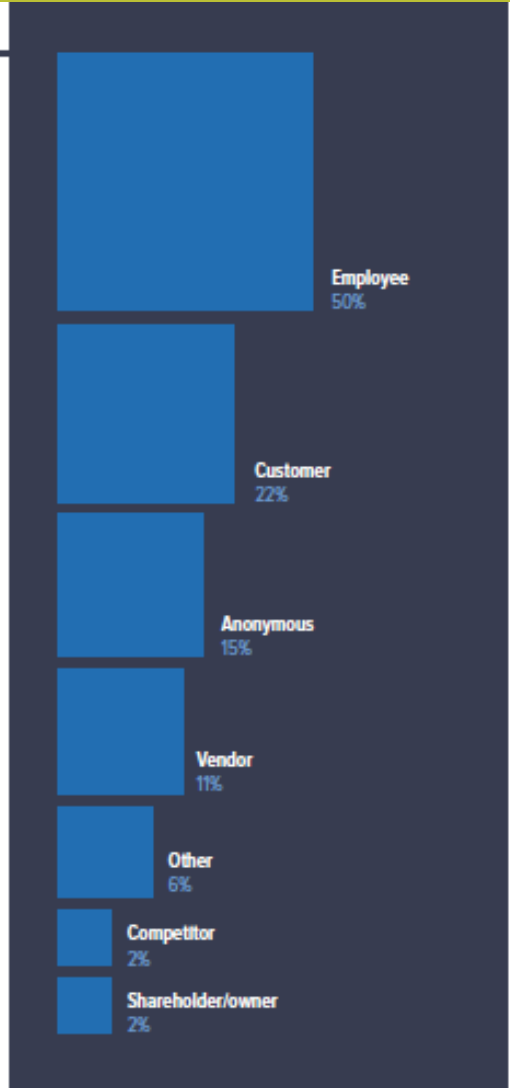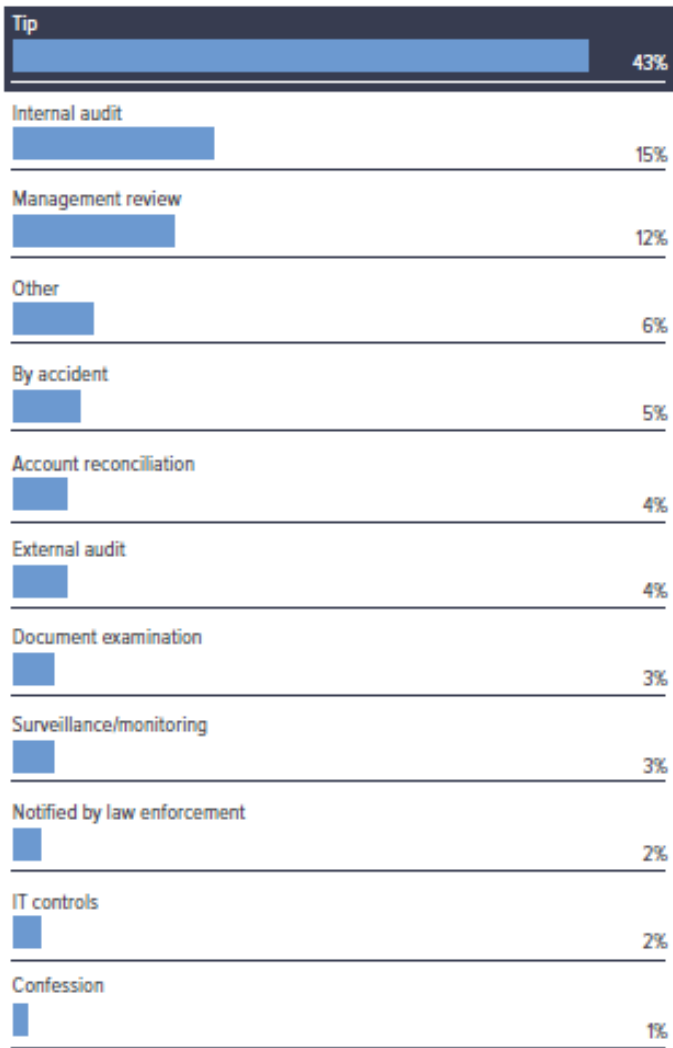
Polling Question

- What percentage of all Fraudsters displayed at least one behavioral red flag while committing their crimes.

  - 25%

  - 65%

  - 85%

  - 95%

Polling Question

Behavioral Red Flags of Fraud

7 KEY WARNING SIGNS

42% Living beyond means

26% Financial difficulties

19% Unusually close association with vendor/customer

15% Control issues, unwillingness to share duties

13% Irritability, suspiciousness, or defensiveness

13% "Wheeler-dealer" attitude

12% Divorce/family problems

Fraud Training Works

Organizations with **FRAUD AWARENESS TRAINING** for employees were **more likely** to gather tips through **FORMAL REPORTING MECHANISMS**

56% of tips with training

37% of tips without training

43% OF SCHEMES WERE DETECTED BY TIP, and half of those tips came from employees

TELEPHONE HOTLINE and **EMAIL** were each used by whistleblowers in **33% OF CASES**
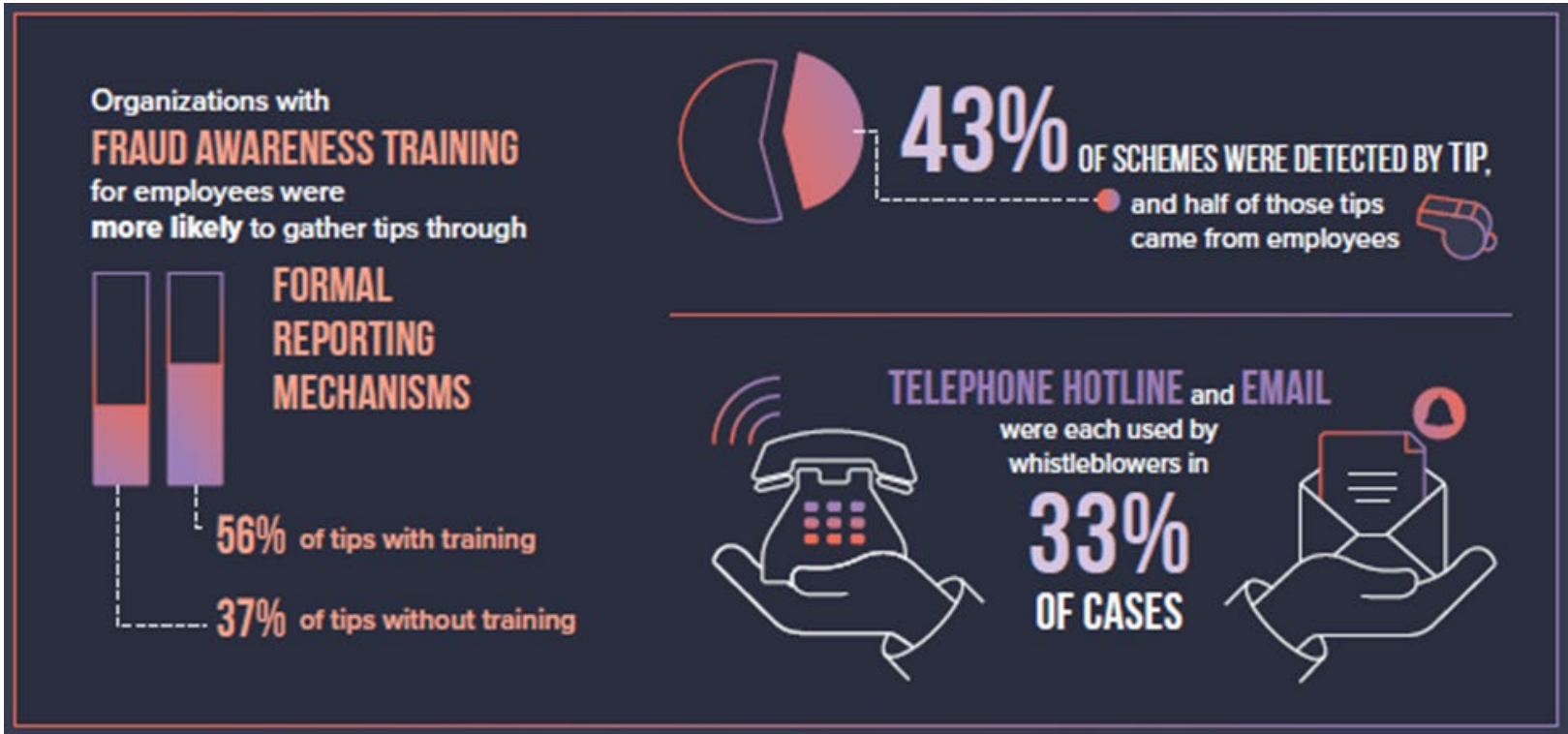
Most Prominent Challenges in Combating Fraud in the Wake of COVID-19

Challenge	August 2020	May 2020
Inability to travel	43%	38%
Challenges in conducting remote interviews	36%	28%
Lack of access to evidence	33%	32%
Canceled or postponed engagements or investigations	31%	35%
Communication challenges or delays	28%	25%
Maintaining data privacy/security	27%	27%
Changes in controls due to remote workforce	27%	26%
Lack of oversight due to remote workforce	26%	22%
Technology challenges	20%	18%
Changes in controls due to staffing changes/reductions	15%	12%
Changes in legal/criminal justice system	13%	14%
Decreased budget for anti-fraud programs or intiatives	13%	9%
Lack of access to professional training	7%	4%
Reduction in anti-fraud staff	6%	6%

6 Steps to Stop or Mitigate Insider Fraud Risks

- Step 1: Update your fraud risk assessment and incorporate new factors emerging from the COVID-19 crisis

- Step 2: Identify, rank and address your risks

- Step3: Upgrade our internal controls, policies and procedures

- Step 4: Communicate and engage the department and auditors

- Step 5: Investigate internal fraud incidents promptly

- Step 6: Report early

Step 1: Update your fraud risk assessment & incorporate new factors emerging from the COVID-19 crisis

- How could a fraudster exploit the recent changes?

  - Phase 2 County Status

  - Modified Lobby Hours

  - Office space modifications in keeping with social distancing

  - Shift to Mail, Phone, Online or Virtual Operations

  - Shift to alternating or all remote work environment

  - Web or electronic communications

  - Operational flux between in person to virtual depending on conditions

  - Limited in person procurement and vendor interactions

  - Modified client direct services interactions and incentives

Step 2: Identify, rank & address your risks

- Identify the changes that have been made due to the new operating environment, for example frequency vs high impact:
    - Shift to online payments
    - Software Overrides Permissions
- Rank them between low and high risk
    - Low chances of occurring Low impact to operations/organization
    - High changes of occurring, High impact to operations/organization
- Develop and design controls to address the changes with higher risk to lower risk-
    - Review of payment reconciliations, exception reporting
- Consider compensating controls if the ideal can't be met
- The selection of controls by management are to be evaluated for their efficiency and effectiveness to ensure that they are not too costly or cumbersome to maintain. Keep in mind that the control should not exceed the benefit to be derived from it.
- Written documentation of risk assessment may be required by regulatory entities both internal and external

Step 3: Upgrade your internal controls, policies & procedures

- Timely Reviews- increase/decrease timelines

- Monitoring- increase/decrease frequency

- Paper to digital documents- validation of digital documents

- Video dual payment processing- record keeping of event

- Signature & Approval, Version Controls- Microsoft Teams

- Update your P&Ps- written document

- Communicate them to your staff, internal & external customers- web page, acknowledgement of receipt

- Significant changes may require prior authorization and approval from regulatory entities both internal and external

Step 4: Communicate and engage the department & auditors

- Ensure that your internal and external customers are aware of the changes in how you operate

  - Emails

  - Signage

  - Webpage updates

  - Webinars/ YouTube

  - Social Media

  - County's FYI

- Significant changes may require consultation with regulatory entities both internal or external

Step 5: Investigate internal fraud incidents promptly

- Great care must be taken when investigating suspected improprieties or irregularities to avoid wrongful accusations or alerting suspected individuals that an investigation is under way. (ACFE)

- Whether a particular act is, in fact, fraud or noncompliance with provisions of laws, regulations, contracts or grant agreements might have to await final determination by a court of law or other adjudicative body. (ACFE)

Step 5: Investigate internal fraud incidents promptly

- Reporting requirement is not intended and should not prevent departments from conducting investigation of known or suspected loss of public assets or from taking appropriate administrative and/or disciplinary action based on the results of an internal investigation.

  - Administrative investigations should be conducted in keeping with adopted Clark County Personal Policy Manual and with BARS 3.10.2.30(4),(5) and 3.10.2.60

- Contact Audit Services and inform them of known or suspected loss

Step 6: Report early

- RCW 43.09.185 requires that all state agencies and local governments immediately notify the State Auditor's Office in the event of a known or suspected loss of public funds or assets or other illegal activity

- Complete and submit form "Report of Loss or Theft"

- Contact Audit Services for guidance

Key takeaways

- Update your fraud risk assessment and incorporate new factors emerging from the COVID-19 crisis

- Identify, rank and address your risks

- Upgrade our internal controls, policies and procedures

- Communicate and engage the department and auditors

- Investigate internal fraud incidents promptly

- Report early

Helpful Resources

- Clark County Auditor's Office

  - (564) 397-4795 or   AuditServices@clark.wa.gov

  - www.clark.wa.gov/auditor

- Information Sources

  - Association of Fraud Examiners

  - https://www.acfe.com/fraud-resources.aspx

  - Six steps to stop or mitigate insider fraud risks

  - https://www.pwc.com/us/en/library/covid-19/mitigate-insider-fraud.html

Thank you!

Comments and questions

GREG KIMSEY, CLARK COUNTY AUDITOR

AUDIT SERVICES
Larry Stafford, Audit Services Manager
Arnold Pérez

1300 Franklin Street Suite 575, P.O. Box 5000, Vancouver, WA 98666-5000

For further information about this contact: Clark County *Audit Services*
Via email *AuditServices@clark.wa.gov* *or phone (564) 397-2310 ext.4795*

###
For other formats, contact the *Clark County ADA Office*: ***Voice*** *(564) 397-2322*
Relay *711 or (800) 833-6388;* ***Fax*** *(360) 397-6165;* ***E-mail*** *ada@clark.wa.gov*