

Prevention of Common Payroll Frauds

Kara Hershberger, CPA, CIA, CISA, CFE –
Manager

Chris Milano, CPA, CFE, CAMS – Consultant

CERTIFIED PUBLIC ACCOUNTANTS
& BUSINESS CONSULTANTS



Agenda

- Learning Objectives (3)
- Payroll Fraud Basics (4)
- Red Flags of Payroll Fraud (12)
- Common Payroll Frauds and How to Stop Them (16)
- Data Analytics (27)
- Payroll Fraud Case Studies (29)
- Why SOC Reports? (38)

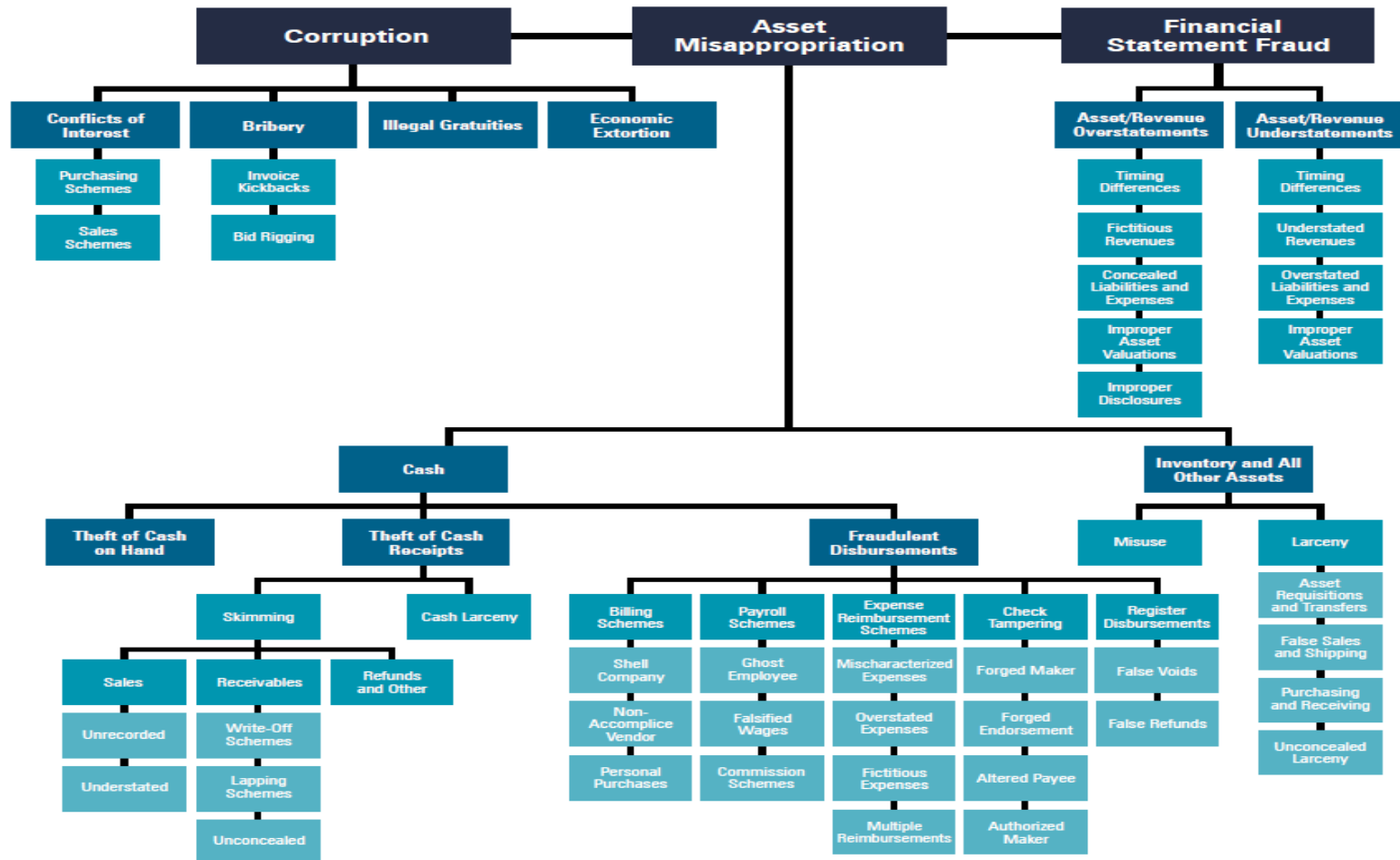


Learning Objectives

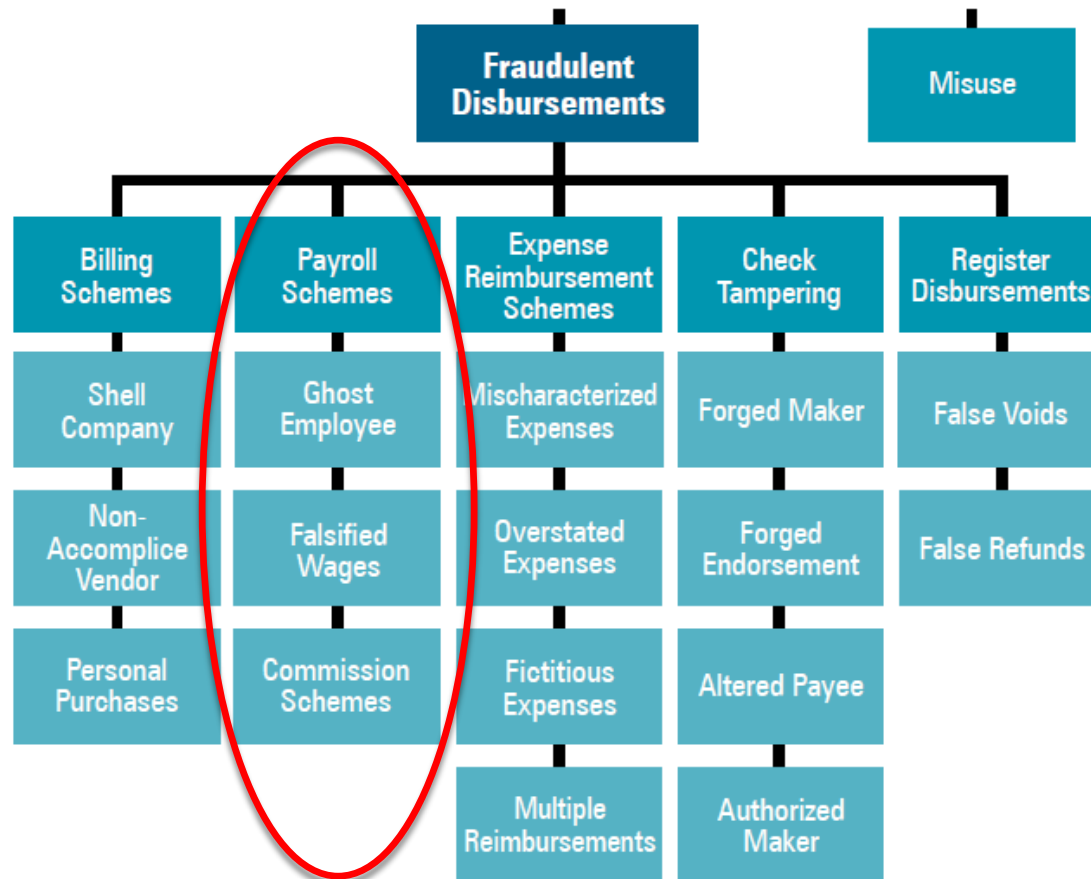
1. List and explain common payroll frauds and internal controls to help prevent those frauds
2. Be able to identify Information Technology general controls for payroll transactions
3. Understand what data analysis tests could identify the red flags of payroll fraud

Types of Fraud

Figure 3: Occupational Fraud and Abuse Classification System (Fraud Tree)



Types of Fraud



Fraud Statistics – Categories

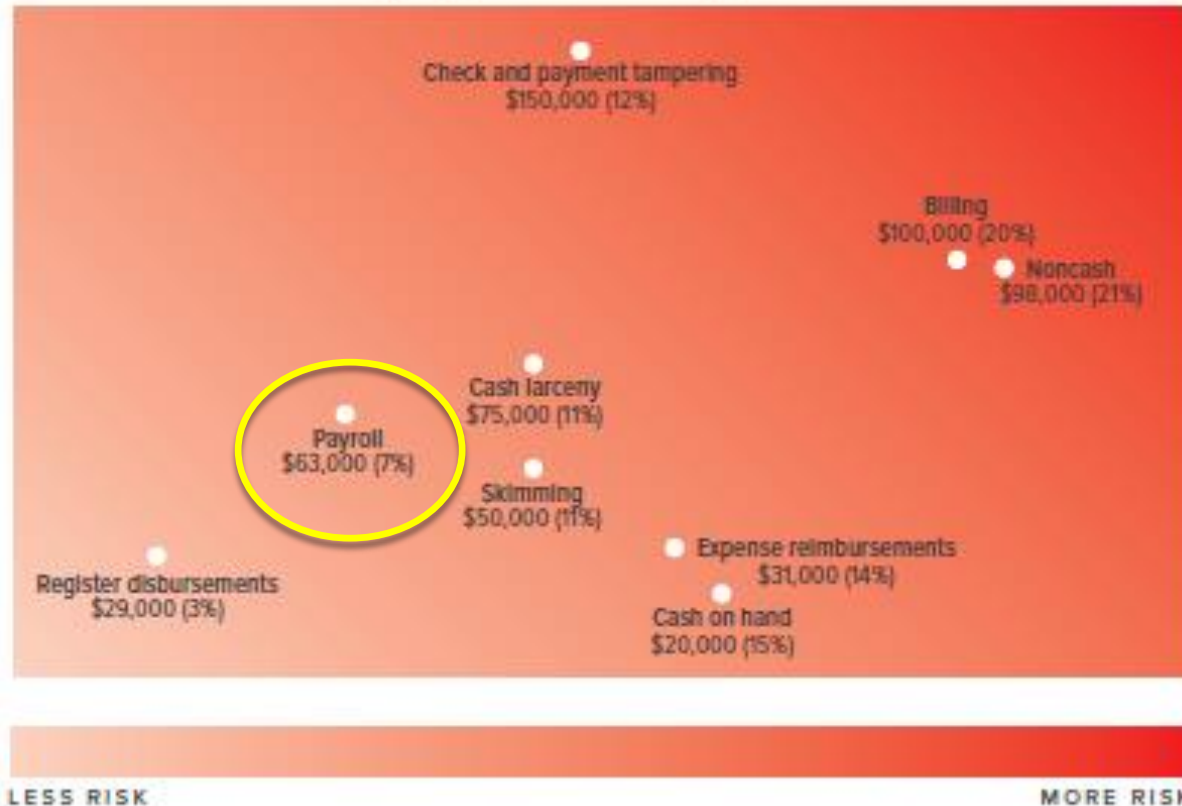
FIG. 3 How is occupational fraud committed?



Source: ACFE Report to the Nations on Occupational Fraud, 2018

Fraud Statistics – Median Loss by Type of Scheme

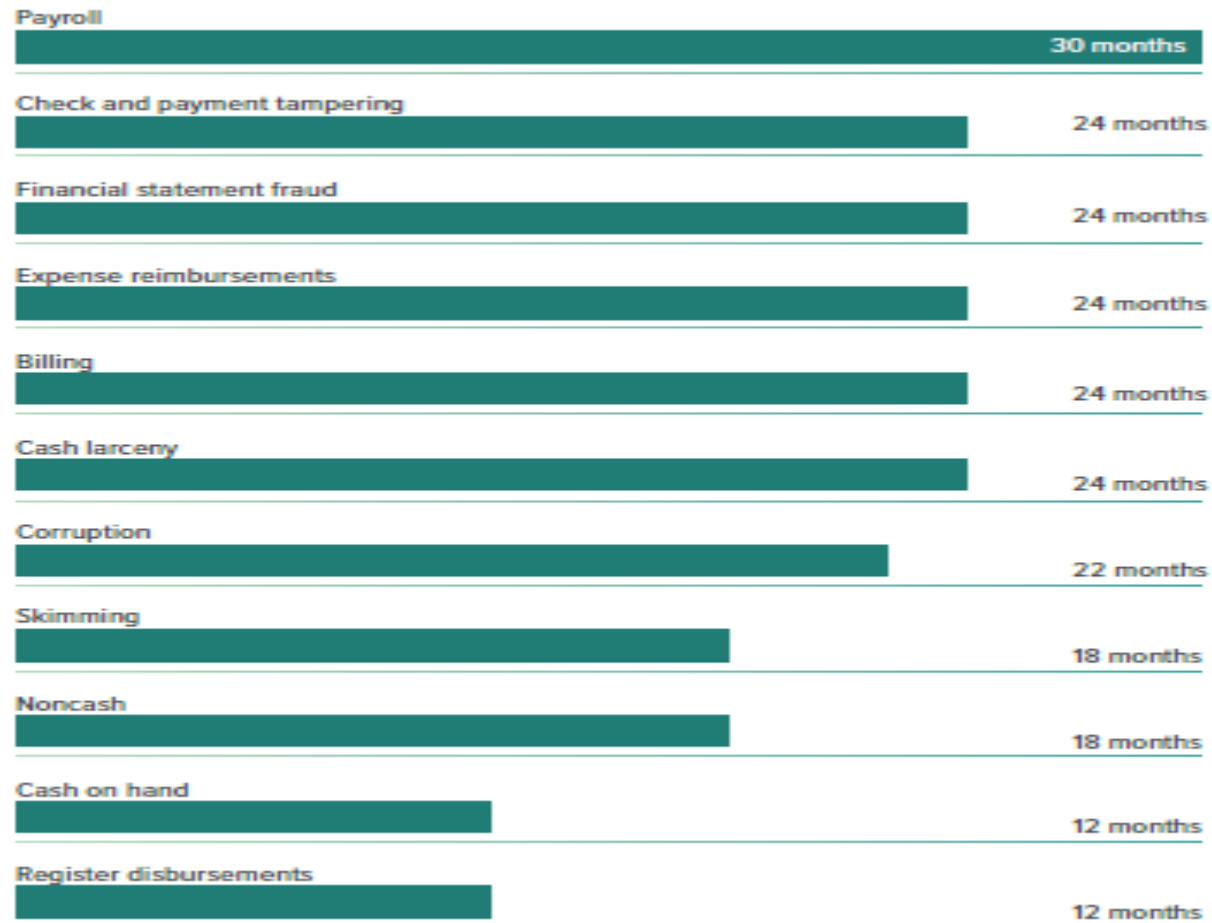
FIG. 6 What asset misappropriation schemes present the greatest risk?



Source: ACFE Report to the Nations on Occupational Fraud, 2018

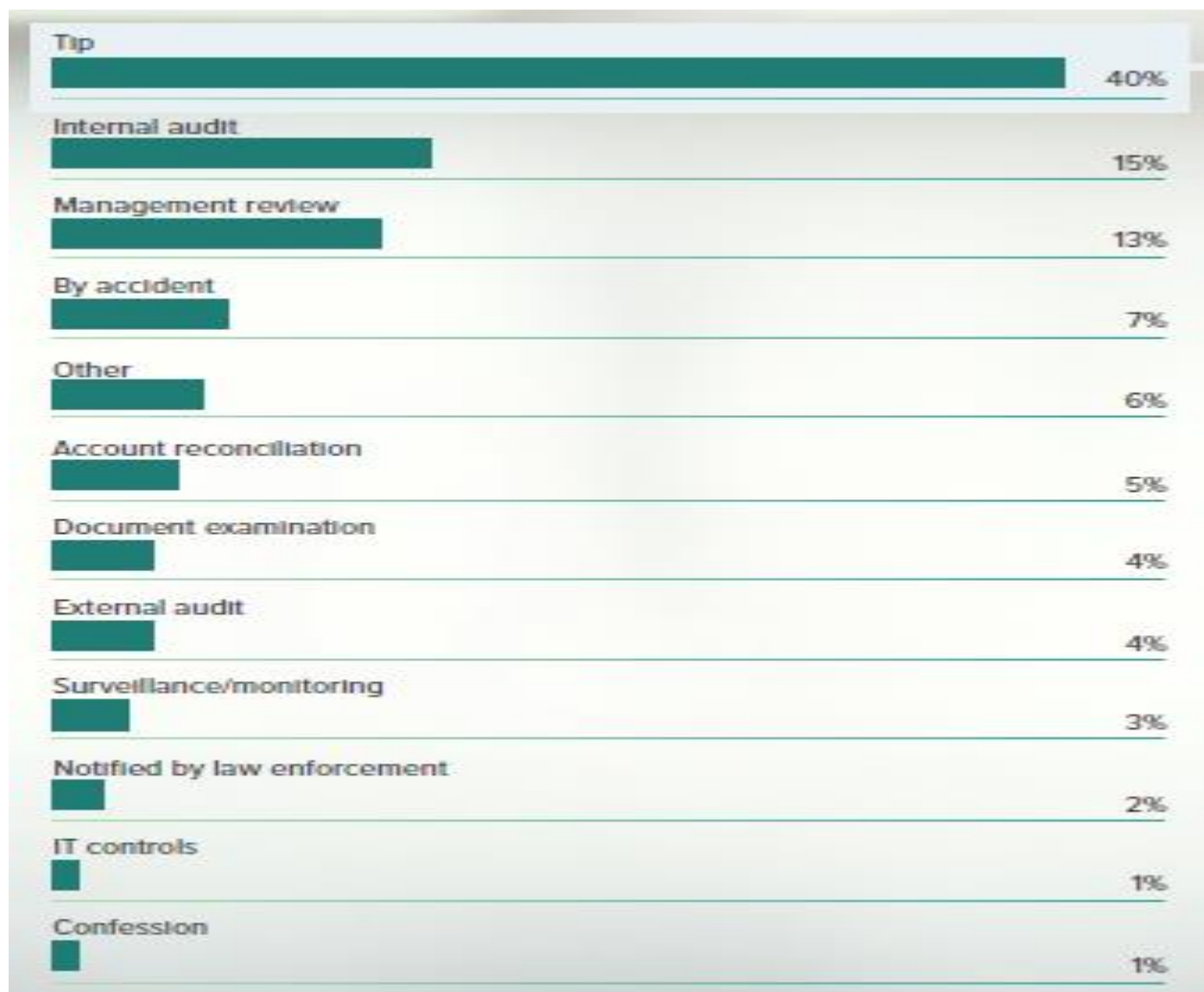
Fraud Statistics – Months to Detection

FIG. 8 How long do different occupational fraud schemes last?



Source: ACFE Report to the Nations on Occupational Fraud, 2018

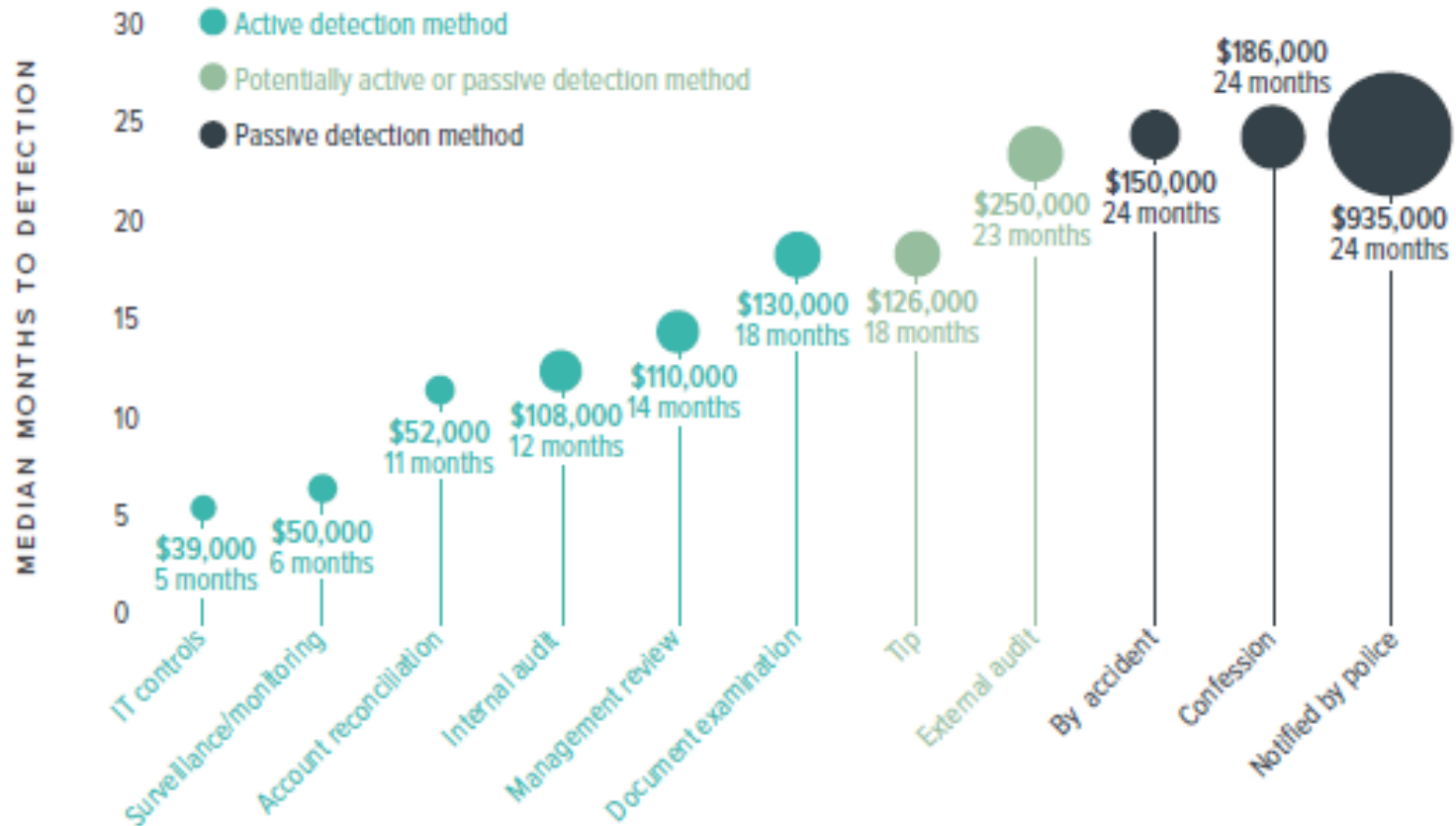
Fraud Statistics – Method of Detection



Source: ACFE Report to the Nations on Occupational Fraud, 2018

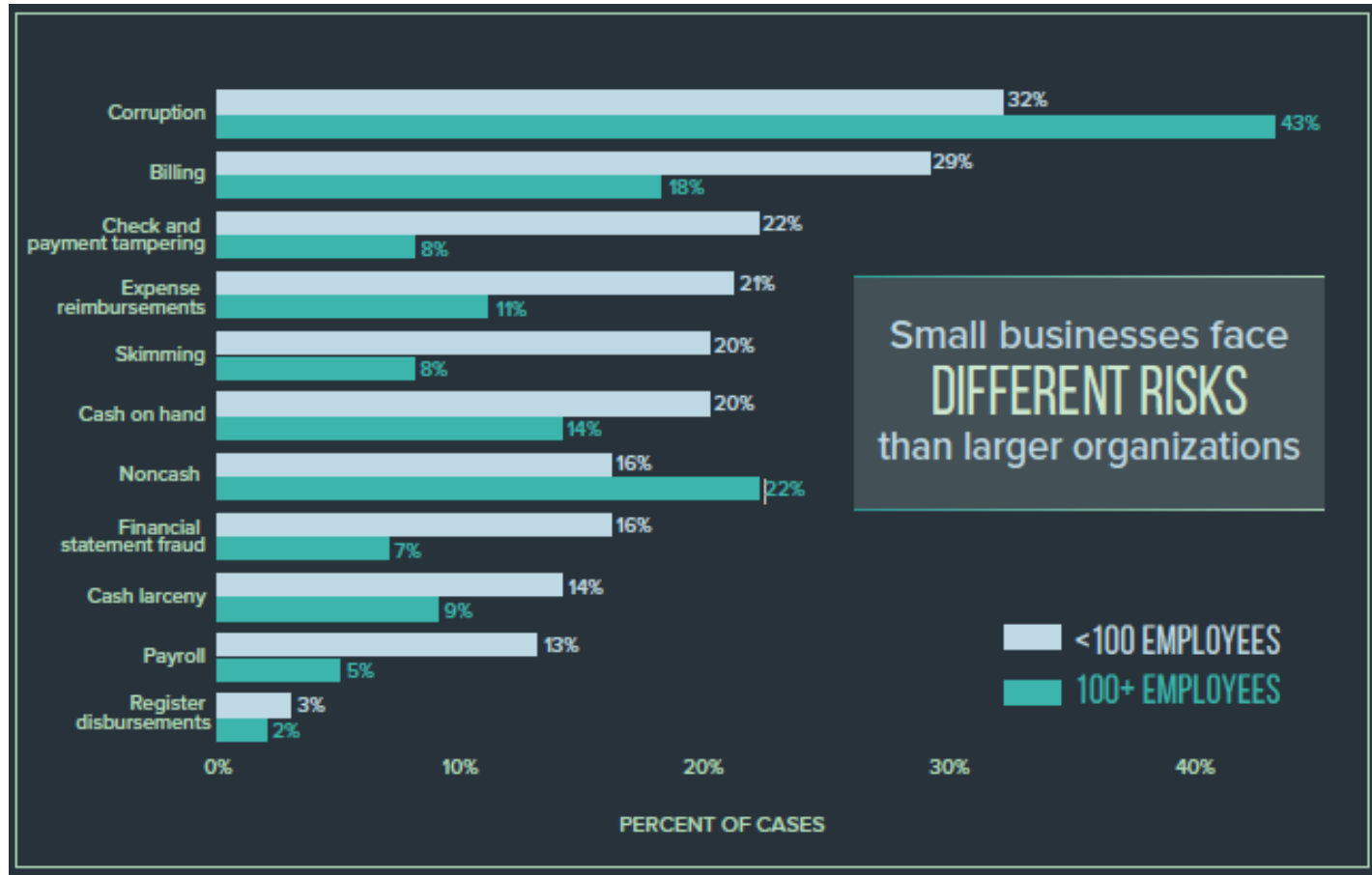
Fraud Statistics – Method of Detection

FIG. 11 How does detection method relate to fraud duration and loss?



Source: ACFE Report to the Nations on Occupational Fraud, 2018

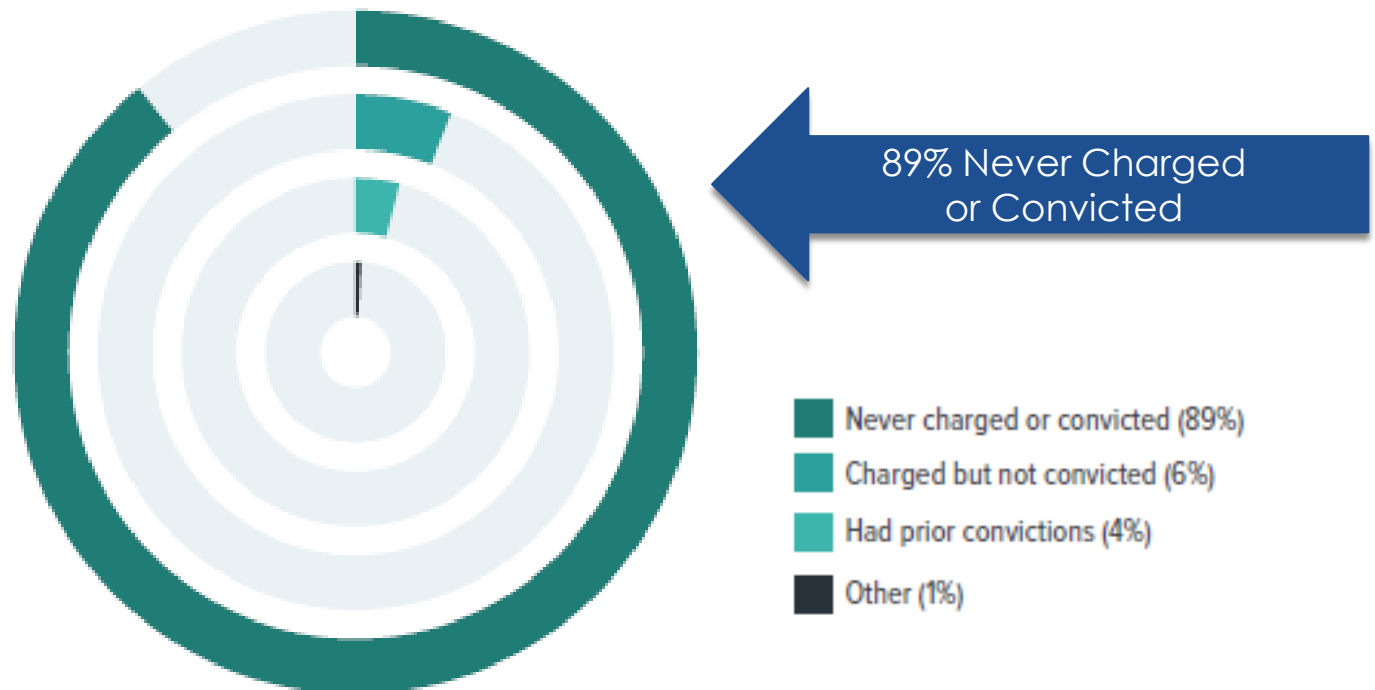
Fraud Statistics – Scheme Type by Size of Organization



Source: ACFE Report to the Nations on Occupational Fraud, 2018

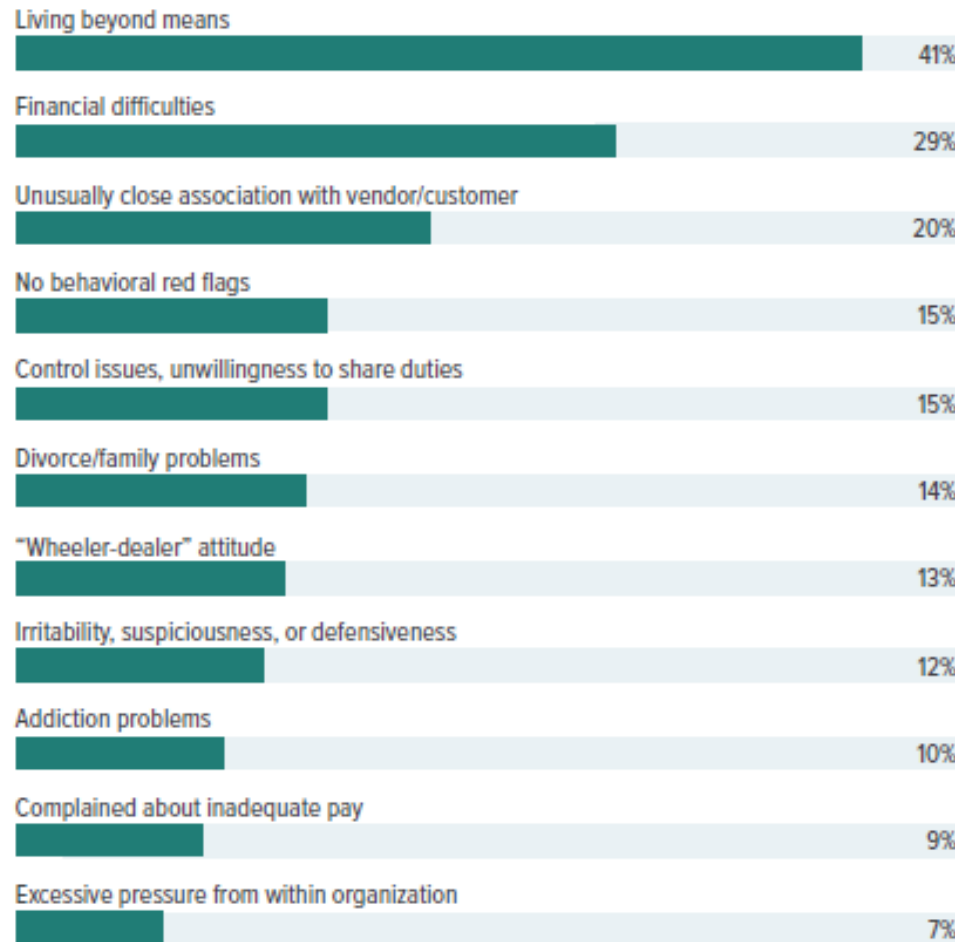
Red Flags - Criminal History of Fraudster

FIG. 36 Do perpetrators tend to have prior fraud convictions?



Red Flags – Behavioral

FIG. 38 How often do perpetrators exhibit behavioral red flags?



Source: ACFE Report to the Nations on Occupational Fraud, 2018

Red Flags – Behavioral

Unexplained Wealth

- Living Beyond One's Means

Sudden Unusual Mood Swings

- HR Problems and Complaints

Problems related to:

- Finances
- Family
- Gambling
- Drug/Alcohol addiction

Red Flags – Payroll Files

Duplicates

- Bank Account for Two Different Employees
- Payments & Time
- Employees with Same SSN #
- Addresses for Two Employees

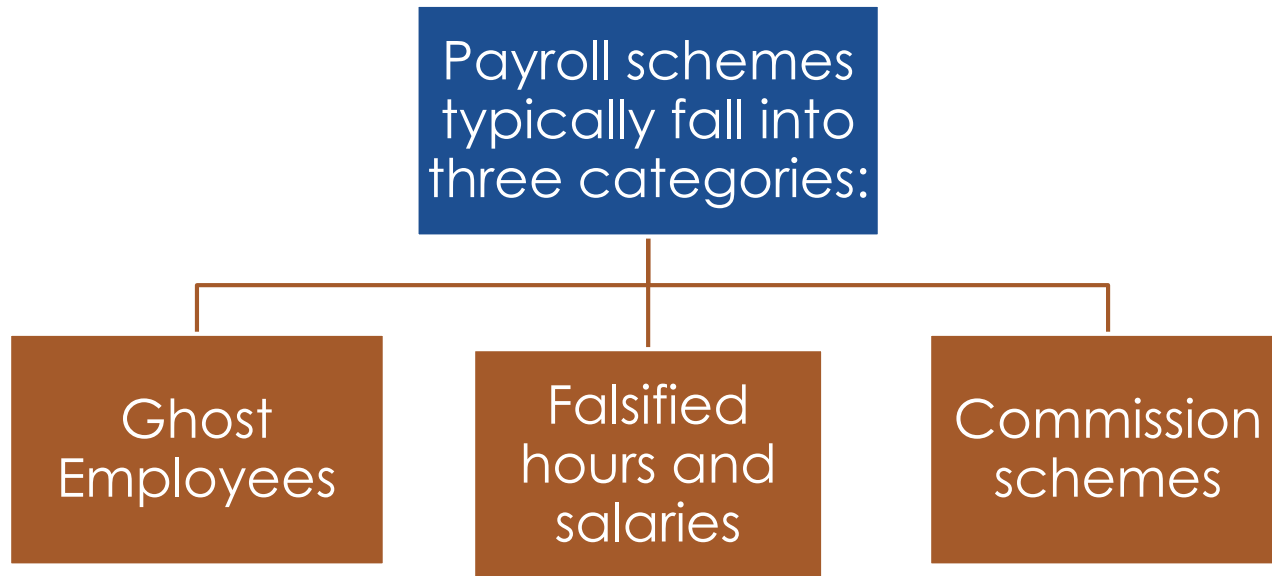
Anomalous Entries

- No deductions (Gross Pay = Net Pay)
- Ex-Employees with Paychecks
- Employees with No Vacation Time Paid
- Oddly timed Pay Increase

Other Items

- Excessive Overtime or Commissions Earned
- Modified Time by Other Employees
- Employees with very Similar Names
- Employees on Payroll that do not appear on HR Listings

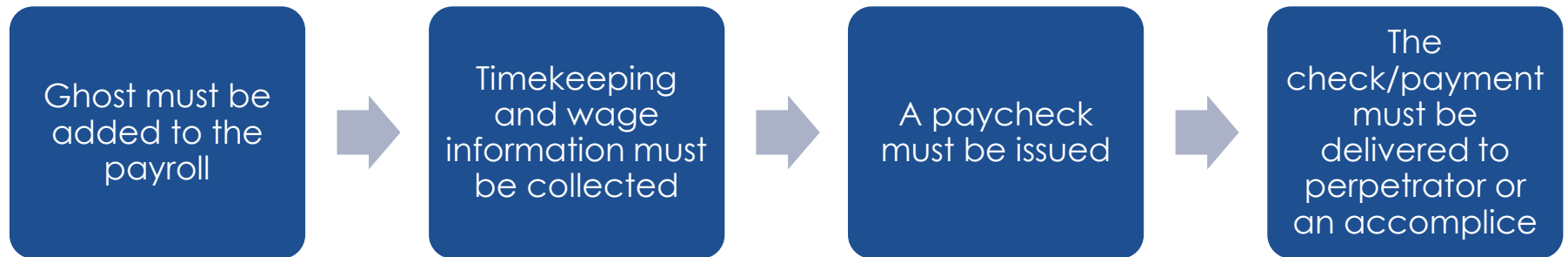
Common Payroll Frauds



- Perpetrators produce false documents which cause a fraudulent disbursement.
 - Falsified timecards
 - Altered payroll records

Payroll Fraud Schemes – Ghost Employees

- For a ghost scheme to work, four things must happen:

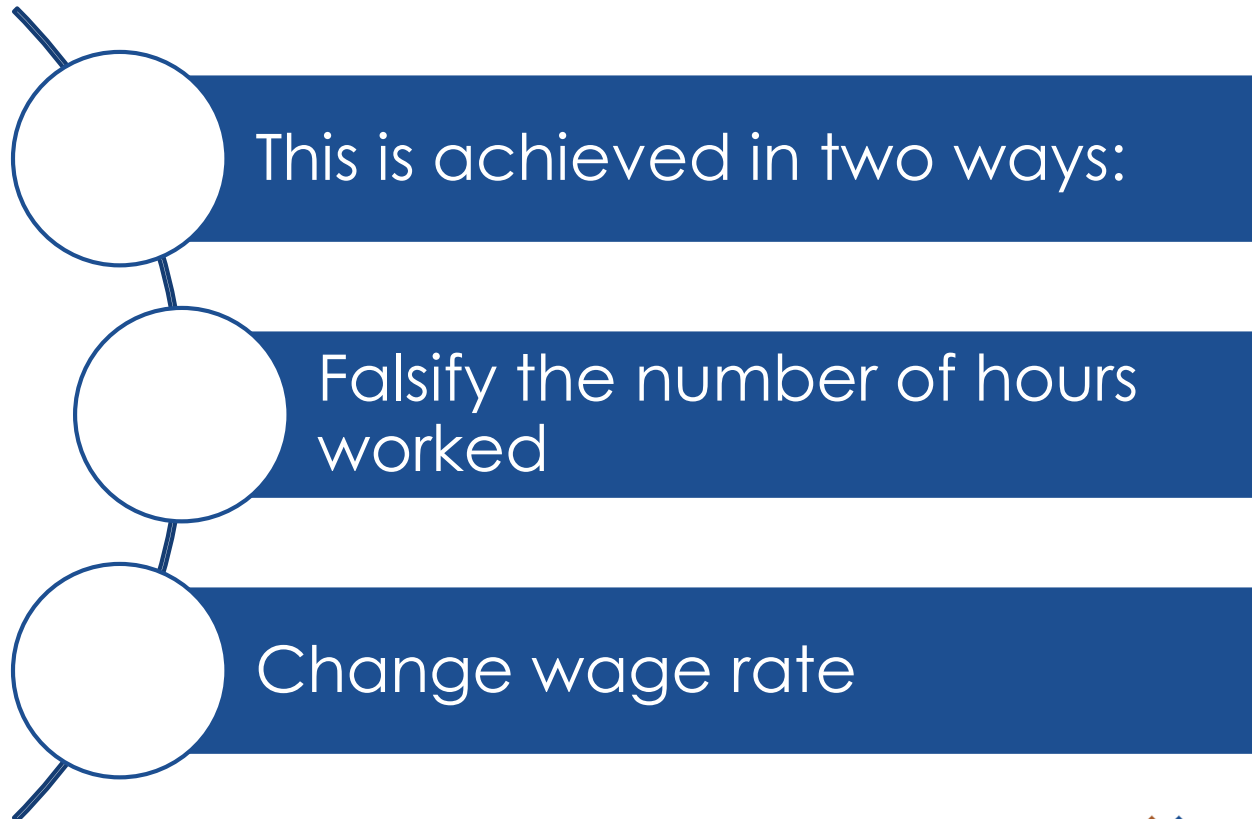


Payroll Controls – Ghost Employees

- Restrict access to add/modify employee data.
- Approvals
 - Changes to payroll data,
 - Supervisory review/approval of all timekeeping.
- Reconciliations
 - Number of employees with supporting documentation,
 - Pay rates with supporting documentation.
- Appropriate review of payroll distribution by employees independent of payroll calculation.

Payroll Fraud Schemes – Falsified Hours or Salaries

- The most common method of misappropriating funds from payroll is overpayment of wages.



Payroll Controls – Falsified Hours or Salaries

- Limit access
 - To change rates of pay,
 - To timekeeping after approval.
- Approvals (Utilize automated workflow where possible)
 - Pay rate changes, hiring, & terminations,
 - Supervisory review/approval of all timekeeping,
 - Executive approval of all bonus-type compensation.





Payroll Controls – Falsified Hours or Salaries

- Reconciliations
 - Separate payroll bank account,
 - Comparison of pay rate changes to payroll records,
 - Hours and salaries paid should be compared to prior periods,
 - Reconciliation to the GL.
- Mandatory vacation for all employees in high risk positions.

Payroll Fraud Schemes – Commission Fraud

There are two ways an employee on commission can fraudulently increase their pay.

-  Falsify the amount of sales
-  Increase their rate of commission

Payroll Controls – Commission Fraud

Commission scheme detection:

- Commission expense should be linearly related to sales figures.
- Comparative analysis of commissions earned.
- Excessive commissions could be a signal of fraud.
- Analyze sales by salesperson for uncollected sales amounts.
- Confirm sales with a random sample of customers.
- Determine if proper segregation of duties for the calculation of commissions exists.

Payroll Controls – Commission Fraud

Segregation of duties for the following:

- Payroll Preparation,
- Payroll Disbursement,
- Payroll Distribution,
- Payroll Bank Reconciliations, and
- Human Resource Department Functions.

Periodic payroll review and analysis.

- Analyze total payroll between periods,
- Analyze number of employees between periods,
- Analyze pay rates between periods.

Payroll Controls – IT General Controls

- User access
 - Unique user authentication
 - User account management
 - Elevated privileges
 - Account access review
- Change management
 - Software acquisitions and updates
 - Data conversions

Payroll Controls – IT General Controls

- IT operations
 - Physical security
 - Third party service providers
 - Backup and restoration
 - Batch processes
- Automated system controls
 - Data input and validation checks

Data Analysis Tests – Do it Yourself Fraud Detection

- Review payroll register for duplicates.
 - Pay checks (same day or pay period),
 - Addresses,
 - SSNs,
 - Bank account numbers,
 - Check numbers.



Data Analysis Tests



Payroll Fraud – Case Studies

- Case Study #1

- Payroll clerk performed multiple functions with SOD issues.
- After the payroll file was sent to the bank, the clerk modified the file to pay fictitious employees.

- Case Study #2

- Employee received more vacation days and vacation buyouts than allowed per the policy

Case Study #1

- Fraudulent payroll scheme detected after an employee was terminated
- A forensic accounting analysis of the fraud was provided for Insurance purposes
 - Fraud occurred from 2005 to 2011
 - Over \$900,000 was stolen

Case Study #1

- How the fraud occurred
 - Payroll clerk performed multiple functions with SOD issues
 - Created payroll disbursements
 - Reconciled payroll account
 - Uploaded payroll information to the GL
 - After the payroll file was sent to the bank, the clerk modified the file to pay fictitious employees.



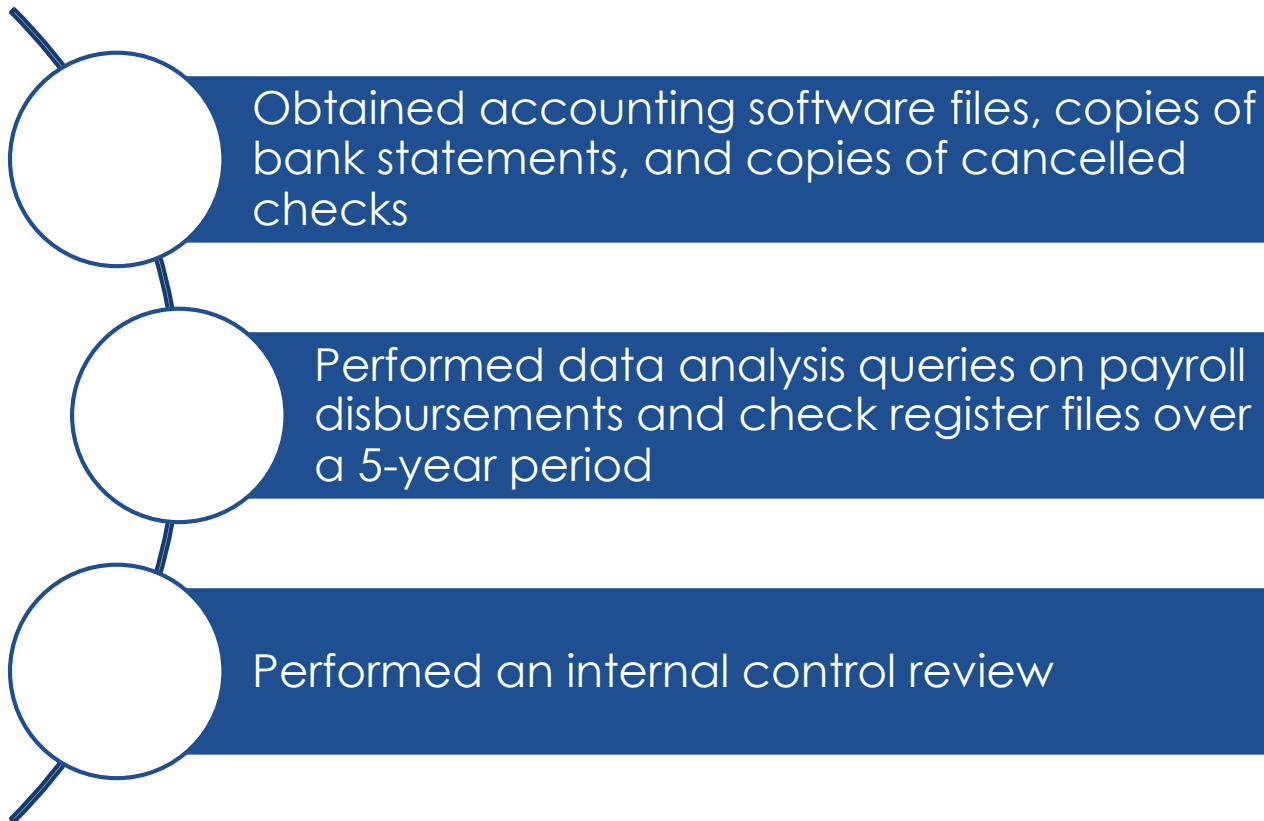
Case Study #1

- Results of the analysis
 - Confirmed fraud took place
 - Confirmed management's assessment of the dollar value of the scheme as \$904,096
 - No reconciliation from the payroll system to the general ledger accounting system occurred. This would have identified the scheme.



Case Study #2

- Suspected misappropriation by Office Manager



Case Study #2

■ Results

- Employee received more vacation days and vacation buyouts than allowed under the company's vacation policy
 - Excess vacation time totaled over \$41,000
- Company funds were used to pay for employee's personal charges
 - Over \$430,000



Case Study #2

■ Results

Category	Total
Personal Credit Cards and Loans	\$ 367,871
Personal Charges on Corporate Credit Cards	64,090
Excess Vacation Time	41,742 - 50,980
Total	\$473,703 - \$482,941

- Provided internal control recommendations
- Findings were presented to Board

Payroll Fraud – California

Former San Francisco Giants Employee Convicted of Fraud

Former Giants Payroll Manager Admits Embezzling \$2.2 Million

U.S. Attorney's Office
November 14, 2011

Northern District of California
(415) 436-7200

SAN FRANCISCO—Robin M. O'Connor pleaded guilty in federal court in San Francisco today to wire fraud, United States Attorney Melinda Haag announced.

In pleading guilty, O'Connor, a former payroll manager for San Francisco Baseball Associates LP, owner of the San Francisco Giants Baseball Club (the Giants), admitted to embezzling approximately \$2.2 million from June 2010 through June 2011. According to the plea agreement, O'Connor diverted money from the Giants and Giants employees by, among other methods, transferring into her personal bank accounts: funds derived from improperly reducing employee tax withholdings, funds intended to pay employee salary and expenses, and funds from fictitious paychecks that she created. O'Connor has returned some of the funds and will forfeit certain assets and pay restitution.

O'Connor, 42, of American Canyon, Calif., was charged by complaint on July 7, 2011, and by information on Nov. 3, 2011. The information charged her with one count of wire fraud in violation of Title 18, United States Code, Section 1343, to which she pleaded guilty pursuant to the plea agreement.

O'Connor was arrested on July 8, 2011, and was released on that date on a \$500,000 secured bond. The sentencing of O'Connor is scheduled for March 5, 2012, before U.S. District Court Judge James Ware in San Francisco. The maximum statutory penalty for a violation of 18 U.S.C. § 1343 is 20 years in prison, and a fine of \$250,000, or twice the gross gain or loss, whichever is greater, plus restitution. However, any sentence following conviction would be imposed by the court after consideration of the U.S. Sentencing Guidelines and the federal statute governing the imposition of a sentence, 18 U.S.C. § 3553.

Thomas E. Stevens is the Assistant U.S. Attorney who is prosecuting the case with the assistance of Rawaty Yim. The prosecution is the result of an investigation by the Federal Bureau of Investigation. The U.S. Attorney's Office acknowledges the valuable cooperation of the Giants in this investigation.

Source: <http://www.fbi.gov/sanfrancisco/press-releases/2011/former-san-francisco-giants-employee-convicted-of-fraud>

Payroll Fraud – Washington

Repeat Embezzler Sentenced to Prison for Stealing More Than \$610,000 from His Employer

*Used Payroll Position to Deposit Payments Labeled for
Former Employees to Own Account*

U.S. Attorney's Office
July 22, 2011

Western District of Washington
(206) 553-7970

ANTHONY G. HILL, 45, most recently from Thurman, Iowa, was sentenced today in U.S. District Court in Seattle to 30 months in prison, three years of supervised release and \$508,354 in restitution for wire fraud. HILL is a former employee in the payroll department of Wireless Advocates, a Seattle cell phone company. Over three years HILL used his access to the company's payroll system to access the accounts of terminated employees, changed the terminated employees' direct deposit account information to an account in his own name, and processed without authorization payroll, commission, bonus, and expense disbursements in the names of those terminated employees. HILL stole \$610,558 using this scheme. At sentencing Chief Judge Robert S. Lasnik noted that HILL had repeatedly engaged in this type of criminal scheme.

According to records filed in the case, between 2006 and 2009, during his employment at Wireless Advocates, HILL changed the direct deposit information for 12 separate terminated employees, and made at least 110 unauthorized direct deposit transactions to his own account. Some of those employees suffered tax consequences because of the false reports of income. HILL's employment at Wireless Advocates was terminated in August 2009, and his replacement uncovered evidence of the scheme. After an extensive internal investigation, the company referred the case to the FBI

Source: <http://www.fbi.gov/seattle/press-releases/2011/repeat-embezzler-sentenced-to-prison-for-stealing-more-than-610-000-from-his-employer>

SOC User Input Considerations

- Service Organization Controls (SOC)
- A SOC report can provide user entities with information about how user-entity information is protected throughout its life cycle.

WHICH SOC IS RIGHT FOR YOUR ORGANIZATION

SOC 1 (SSAE 16) - A SOC 1 is a report on controls at a service organization that may be relevant to user entities' internal control over financial reporting.

SOC 2 - A SOC 2 report is based on the existing SysTrust and WebTrust principles. The purpose of a SOC 2 report is to evaluate an organization's information systems relevant to security, availability, processing integrity, confidentiality or privacy.

SOC 3 - A SOC 3 report, like SOC 2, is based on the existing SysTrust and WebTrust principles. The difference being, the report does not detail the testing performed and is meant to be used as marketing material.

SOC User Input Considerations

- Identify and test controls over activities of a service organization
- Identify and test controls over data provided to service organizations
 - Accuracy of data
 - Completeness of data



Questions

