Insider Threat Vulnerabilities to Consider in Fraud

Presented by:

Alan E. Small MBA, CIA, CFE, CCA, LTP

October 19, 2018

***With references to the Association of Certified Fraud Examiners and the Institute of Internal Auditors**

Insider Threat Vulnerability

- Insider Threat Vulnerability (ITV) creates a pathway for the opportunist to access targeted sources of records from an inventory of files arranged into categories that contain operating footprints of organizational plans exposing the weaknesses of the internal control environment. An opportunist will take advantage of these weaknesses.*

- A. E. Small*

- In all organizations, internal and external threat exposure can result in fraud and originates with underdeveloped business control practices. These exposures drive the heartbeat of every organization affecting hiring, communications, financial management, taxes, procurement, physical plant, security transportation, and food services operations. Such vulnerabilities weaken financial stability and become insider threats to the going concern opportunities for business success. A prescription of internal auditing and fraud assessment may serve business well to minimize the effects of these threats.*

- A.E. Small*

What is Fraud?

"… **any illegal act characterized by deceit, concealment, or violation of trust**. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage."

IIA's International Professional Practices Framework (IPPF)

Definition of Fraud

Maryland Code

- **2010 Maryland Code**
  CRIMINAL LAW
  TITLE 8 - FRAUD AND RELATED CRIMES
  Subtitle 5 - Public Fraud
  Section 8-501 - "Fraud" defined.
- **§ 8-501. "Fraud" defined.**

- In this part, "fraud" includes:
- (1) the willful making of a false statement or a false representation;
- (2) the willful failure to disclose a material change in household or financial condition; or
- (3) the impersonation of another.

- [An. Code 1957, art. 27, § 230A(b)(1); 2002, ch. 26, § 2.]

Association of Certified Fraud Examiners

- Black's Law Dictionary defines fraud as:
- All multifarious means which human ingenuity can devise, and which are resorted to by one individual to get an advantage over another by false suggestions or suppression of the truth. It includes all surprises, tricks, cunning or dissembling, and any unfair way by which another is cheated.

What Is Fraud?

Fraud is a silent crime

There are no exciting chase scenes, no smoking guns, and no bleeding victims.

Fraud however cost billions of dollars in damage.

Focus is Occupational Frauds

Stealing money or inventory

Taking kickbacks or bribes from vendors or customers

Falsifying internal reports

Filing false reports

Using company assets without permission

Withholding information from internal auditors about major events that could impact business, such as obsolete products or pending lawsuits.

What Causes People to Commit Fraud

-Pressure-

A gambling or Drug Habit
Personal Debt or Poor Credit
Peer or Family Pressure to Succeed.

-Opportunity-

Access to records
Situational Timing

-Rationalization-

They owe it to me
I deserve this after the way I’m treated

Association of Certified Fraud Examiners

How to Document an Insider Threat Potential Fraud

Develop the fraud theory

-Who might be involved?
-Why might the allegation be true?
-Where might the fraud be concealed?
-When did the suspected fraud take place?
How is the fraud being perpetrated?

How to Document a Potential Fraud for Investigation

-Determine the location of the evidence

-Is the evidence direct or circumstantial?

-Identify potential witnesses

What evidence is necessary to support intent?

-Number of occurrences

-Other areas of impropriety

-Witnesses

How to Document a Potential Fraud for Investigation

-Revise the investigation theory

-Prepare a chart for linking people and evidence

The Institute of Internal Audit's Fraud-related Standards

Internal auditors must:

- "....**have sufficient knowledge** to evaluate the risk of fraud...." (IPPF 1210.A2)
- **"....exercise due professional care**...." (IPPF 1220.A1)
- "CAE must **report periodically** to senior management and the board ..... **on fraud risks**...." (IPPF 2060)

The IIA’s Fraud-related Standards

Internal auditors must:

- “....**evaluate the potential for the occurrence of fraud** and the **manner in which the organization manages fraud risk**.” (IPPF 2120.A2)
- “....**consider the probability of significant** errors, **fraud**, noncompliance, and other exposures when developing the engagement objectives.” (IPPF 2210.A2)

Types of Fraud

Asset Misappropriation

- Misappropriations are those schemes in which the employee steals or misuses an organization's assets.

Corruption

- Corruption schemes involve a fraudster wrongfully using their influence in a business transaction for the purpose of obtaining a benefit for himself or another person.
- Examples include conflicts of interest, accepting illegal gratuities, and bribery.

Independent Contractor Fraud

Scenario	Fraud
An IT consultant under contract **illegally accesses the company's computer systems .** Source: U.S. Department of Justice, Computer Crime and Intellectual Property Section	After the company declined to offer an IT contractor permanent employment, **he illegally accessed the company's computer systems and caused damage by impairing the integrity and availability of data**. He was indicted on federal charges, a charge that carries a maximum statutory penalty of 10 years in federal prison.

Access to systems or data for personal gain

Scenario	Fraud
A database analyst for a major check authorization and credit card processing company, **exceeds his authorized computer access** . Source: U.S. Department of Justice, Computer Crime and Intellectual Property Section	The employee **uses his computer access to unlawfully steal consumer information of 8.4 million individuals.** The information stolen included names and addresses, bank account information , and credit and debit card information. He sold the data to telemarketers over a five year period. **A U.S. District Judge sentenced him to 57 months' imprisonment and a $3.2 million** in restitution for conspiracy and computer fraud

Access to systems or data for personal gain

Scenario	Fraud
A database analyst for a major check authorization and credit card processing company, **exceeds his authorized computer access** . Source: U.S. Department of Justice, Computer Crime and Intellectual Property Section	The employee **uses his computer access to unlawfully steal consumer information of 8.4 million individuals.** The information stolen included names and addresses, bank account information , and credit and debit card information. He sold the data to telemarketers over a five year period. **A U.S. District Judge sentenced him to 57 months' imprisonment and a $3.2 million** in restitution for conspiracy and computer fraud

Access to systems or data for personal gain

Scenario	Fraud
An employee in the payroll department **moved to a new position**. Upon switching positions, the employee's **access rights were left unchanged**. •Source: 2008 Insider Threat Study, US Secret Service and CERT/SEI	Using the retained privileged access rights, the employee **provided an associate with confidential information** for 1,500 of the firm's employees, including 401k account numbers, credit card account numbers, and social security numbers, which was then used to commit over 100 cases of **identity theft**. The insider's actions caused over **$1 million in damage** to the company and its employees.

Changes to system programs or data for personal gain

Phase	Fraud	Oversights
Requirements Definition	**195 illegitimate drivers' licenses were created and sold** by a police communications officer who accidentally discovers she can create them.	Ill-defined authentication and role-based access control requirements. Ill-defined security requirements for automated business processes. Lack of segregation of duties.

Source: 2008 Insider Threat Study, US Secret Service and CERT/SEI

Changes to system programs or data for personal gain

Phase	Fraud	Oversights
System Design	An employee realizes there is no oversight in his company's system and business processes, so he works with organized crime to enter and profit from **$20 million in fake health insurance claims.**	Insufficient attention to security details in automated workflow processes. Lack of consideration for security vulnerabilities posed by authorized system overrides.

Source: 2008 Insider Threat Study, US Secret Service and CERT/SEI

Changes to system programs or data for personal gain

Phase	Fraud	Oversights
System Maintenance	A foreign currency trader covers up losses of $691 million over a five-year period by making **unauthorized changes to the source code.**	Lack of code reviews. End-user access to source code.

Source: 2008 Insider Threat Study, US Secret Service and CERT/SEI

Changes to system programs or data for personal gain

Phase	Fraud	Oversights
System Maintenance	A foreign currency trader covers up losses of $691 million over a five-year period by making **unauthorized changes to the source code.**	Lack of code reviews. End-user access to source code.

Source: 2008 Insider Threat Study, US Secret Service and CERT/SEI

IT Fraud Risk Assessment - Example

Business Owner-	Fraud Risks	Controls	Preventive or Detective	Monitoring	Likelihood	Impact
IT - CIO	Access to systems or data for personal gain. (Logical Access) Access to customers' or employees' personal information (e.g., credit card information, payroll information) Access to confidential company information (e.g., financial reporting, supplier data, strategic plans) Copying and use of software or data for distribution	Identity management (e.g. individual user IDs, automated password complexity rules, password rotation) Access controls Authentication controls Authorization controls Access control lists Network controls Anti-virus and patch management Restricted access to software code	Both	Information security System administrators Business owners Internal auditing	Medium	High

Institute of Internal Auditors

- The Institute has developed a process for auditing Insider Threat Programs. It includes building a insider threat profile that includes:

IT sabotage Theft of IP

Former employee Current employee

Computer network Trade secrets

Malice (revenge) Financial gain

Disruption to operations Loss of competitive advantage

Institute of Internal Auditors

- **Planning Engagements to Assess Insider Threat Programs**

- Standard 2200 – Engagement Planning instructs that internal auditors must develop and document a plan for each engagement. Standard 2201 – Planning Considerations adds that internal auditors must consider:
- The strategies and objectives of the activity being reviewed and the means by which the activity controls its performance. The significant risks to the activity's objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level. The adequacy and effectiveness of the activity's governance, risk management, and control processes compared to a relevant framework or model. The opportunities for making significant improvements to the activity's governance, risk management, and control processes.
- Engagement planning typically includes several steps that help internal auditors gain an understanding of the area or process that will be reviewed and document the information that supports the engagement plan and work program. Because reviewing and documenting information is an ongoing process, the steps may not be completely distinct and linear.

Institute of Internal Auditors

- **Understanding the Process or Area Under Review**

- There are two critical areas the internal auditor must understand clearly when planning an engagement to assess how well the organization is managing risks related to insider threats. Internal auditors should first understand the nature of insider threats and the practices that may be implemented to identify, protect, detect, respond to, and recover from an IT security incident. To build their knowledge, internal auditors may consider using established security frameworks, programs, and recommendations. Appendix E lists resources and agencies that provide guidance and assistance related to information security, and Appendix F offers additional resources. Internal auditors may start with this information but should identify specific frameworks and recommendations applicable to the industry, market, and geographical location in which their organization operates.
- In addition, internal auditors should understand the organization and its objectives. Understanding the business objectives provides a basis for internal auditors to identify risks that should be included in the preliminary engagement-level risk assessment (as required by Standard 2210.A1).

Institute of Internal Auditors

- **Developing an Insider Threat Program**

- To improve the rate of success, the organization should formalize the program and manage its development and implementation in a systematic way (similar to any other project) that clearly documents expectations, roles and responsibilities, timing and activities. By having a formal project plan or road map, the organization can identify the current state (gap analysis) and determine the resources needed to complete the project (e.g., people, money, time, and technology). One key to a successful insider threat management process is collaboration among functions that provide oversight (e.g., senior management and the board) and those responsible for implementing the program (e.g., human resources, legal, operations, data owners, information security, and software engineering).
- Rather than starting from the ground up, organizations can benefit from customizing existing insider threat management frameworks developed by private, public and not-for-profit organizations to fit their specific needs. By doing so, the organization can speed the development and implementation of the insider threat program.

FIG. 1 **Countries with reported cases and median loss for each region**

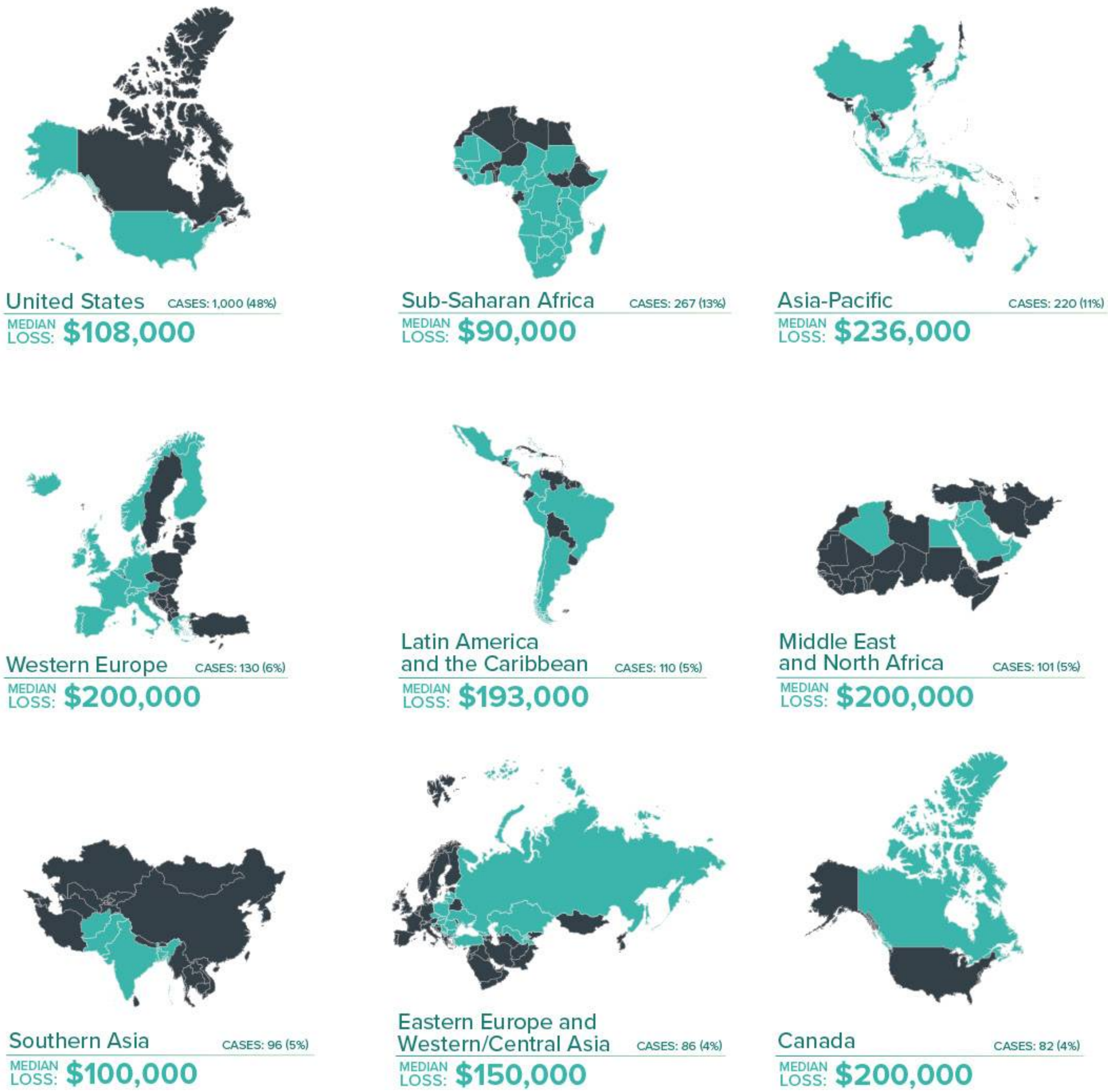


FIG. 2 **How much does an occupational fraud cost the victim organization?**

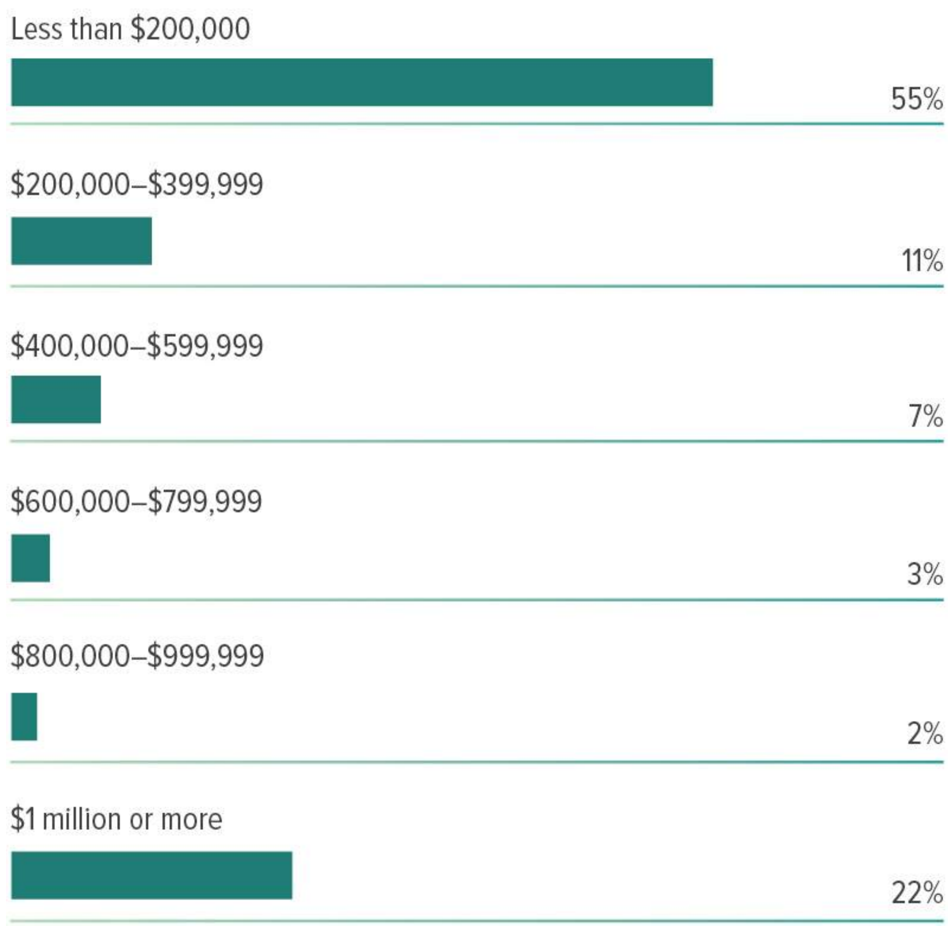


FIG. 3 **How is occupational fraud committed?**

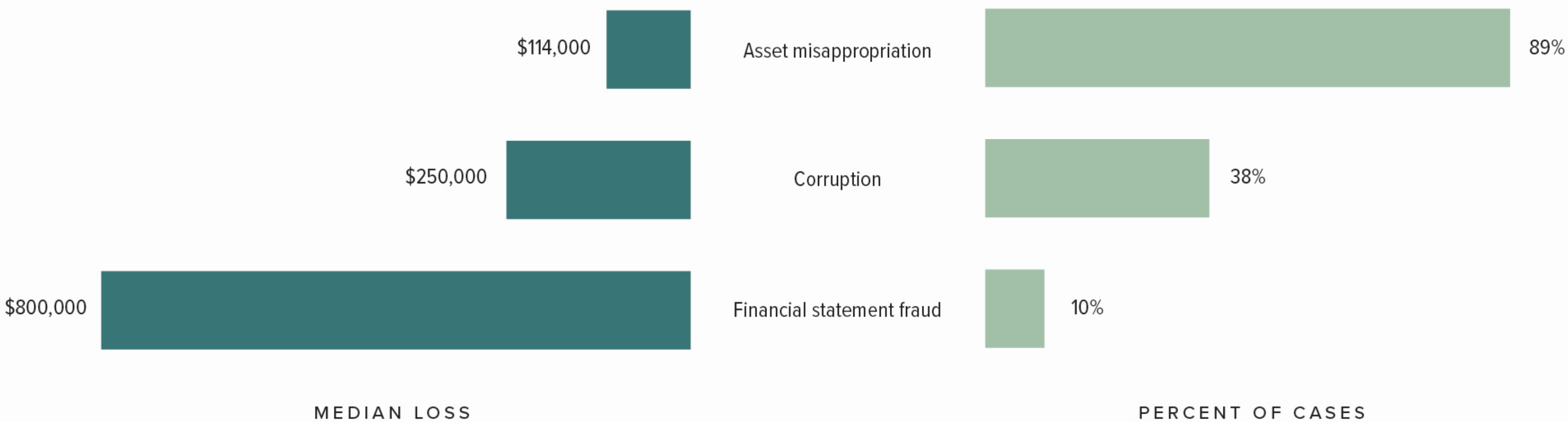


FIG. 4 **Occupational Fraud and Abuse Classification System (the Fraud Tree)**

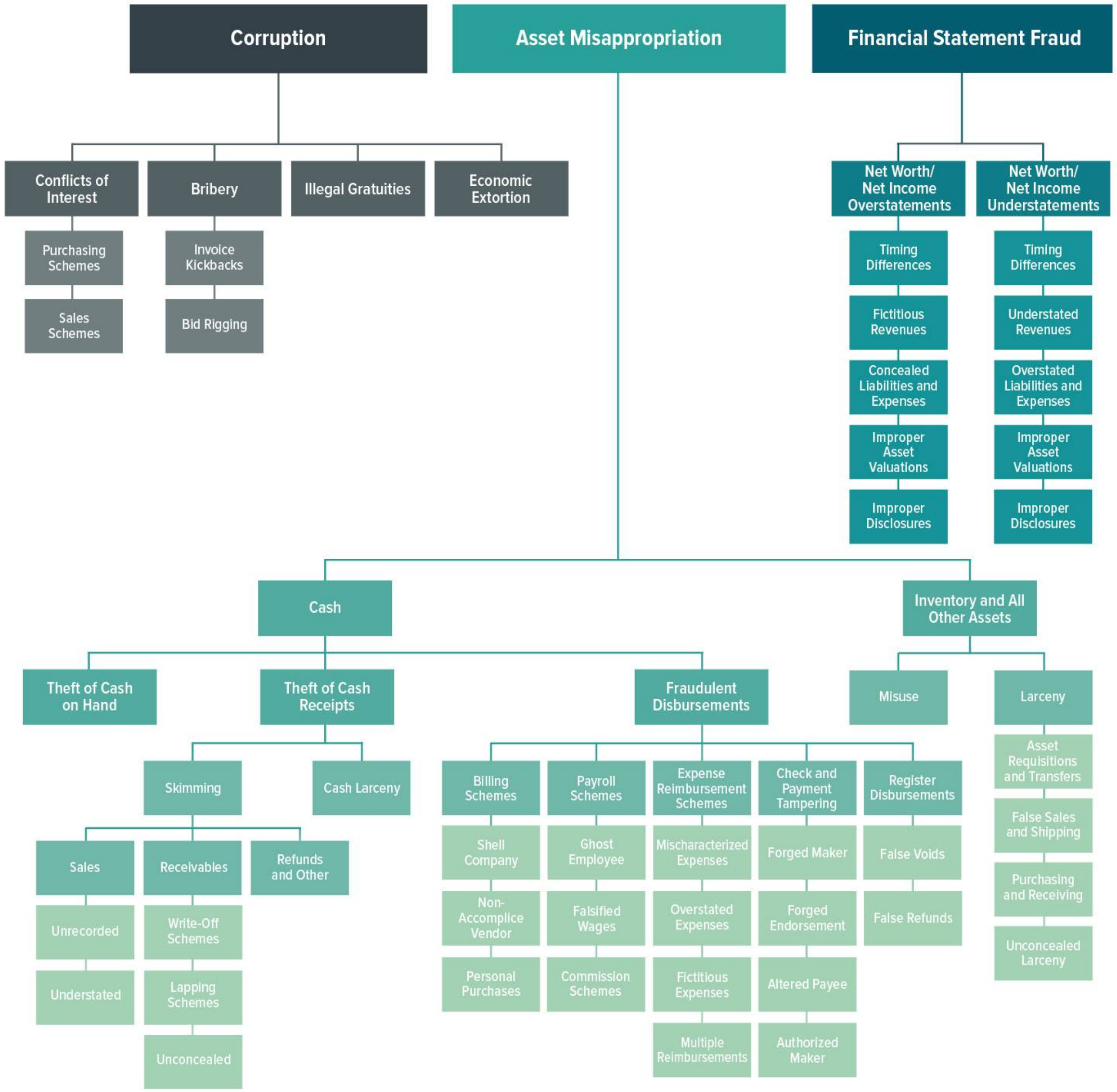


FIG. 9 **How is occupational fraud initially detected?**

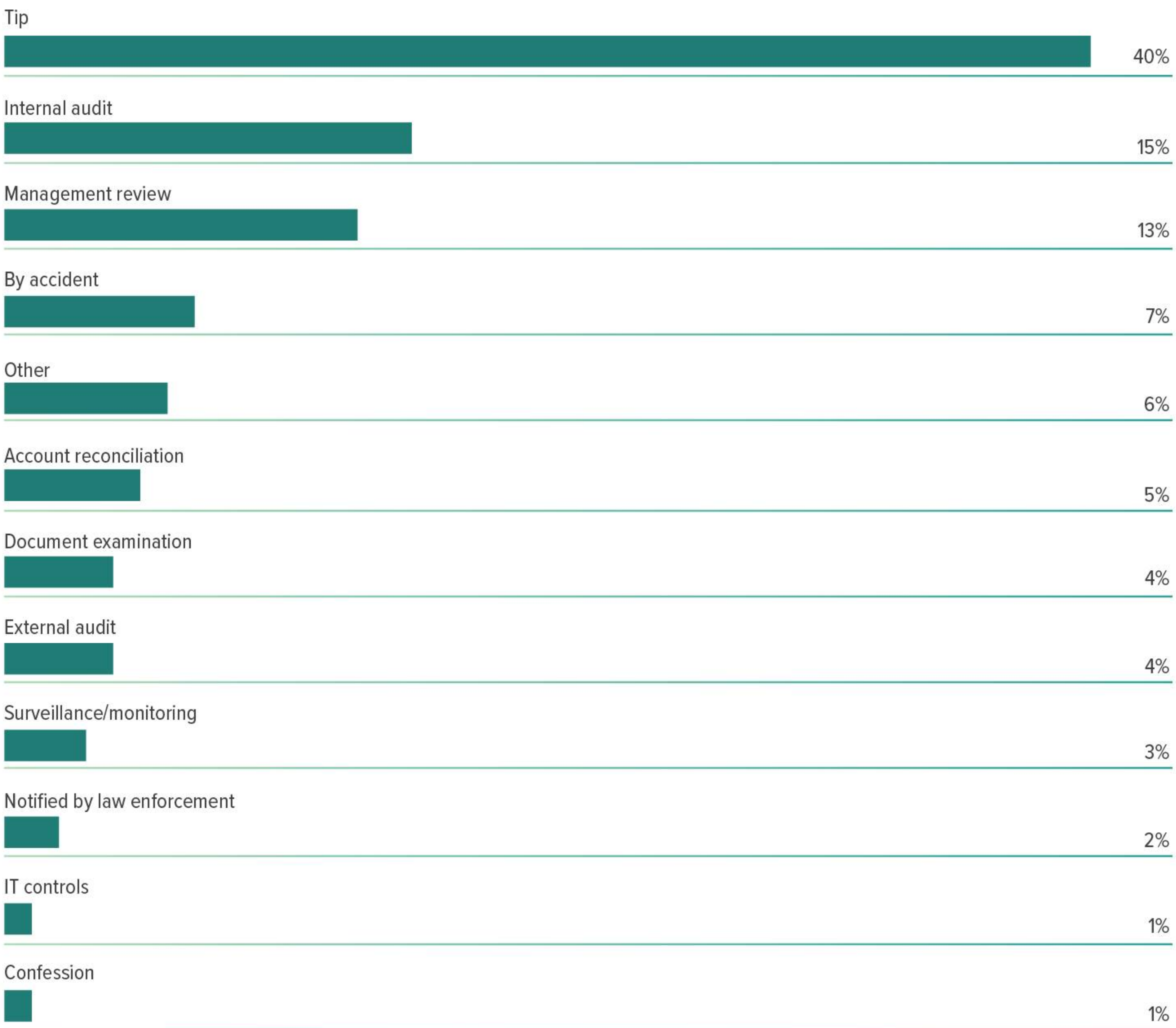


FIG. 10 **Who reports occupational fraud?**

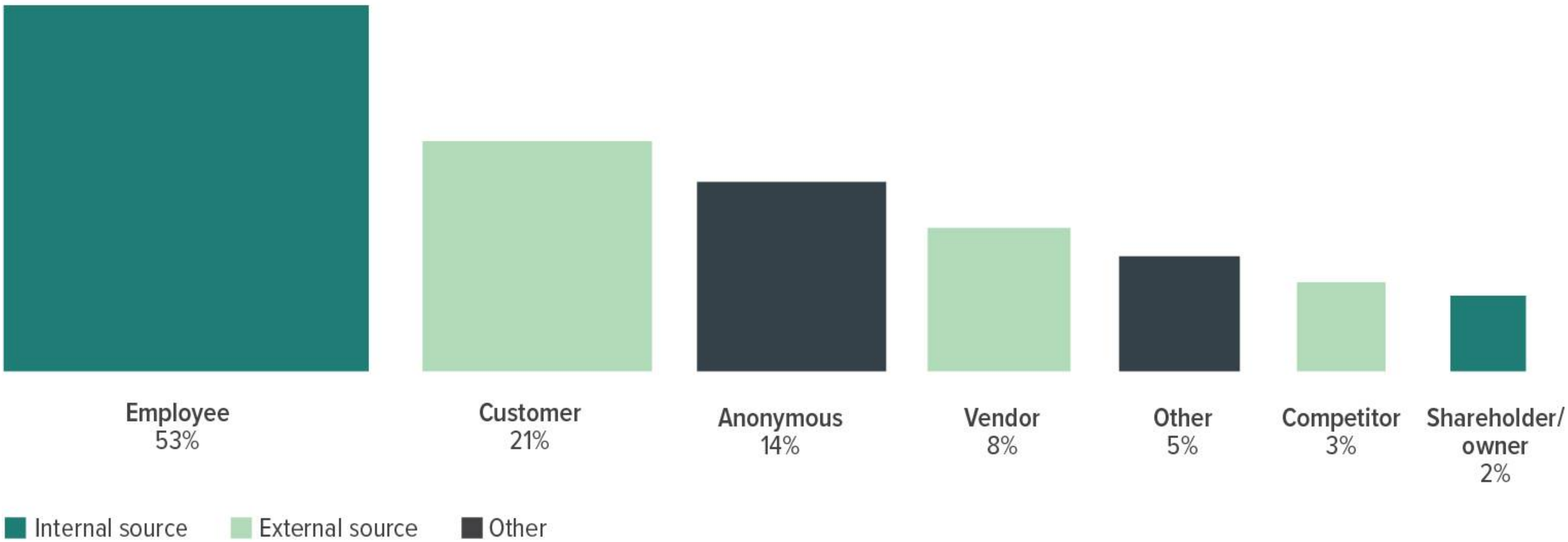


FIG. 15 **How does occupational fraud affect organizations in different industries?**

Industry	Cases	Median loss
Banking and financial services	366	$110,000
Manufacturing	212	$240,000
Government and public administration	201	$125,000
Health care	158	$100,000
Retail	108	$50,000
Insurance	101	$153,000
Education	97	$68,000
Energy	94	$300,000
Construction	90	$227,000
Other	84	$70,000
Transportation and warehousing	83	$140,000
Food service and hospitality	76	$90,000
Technology	68	$150,000
Religious, charitable, or social services	60	$90,000
Services (professional)	58	$258,000
Arts, entertainment, and recreation	51	$88,000
Telecommunications	50	$100,000
Real estate	35	$180,000
Agriculture, forestry, fishing, and hunting	32	$136,000
Utilities	29	$150,000
Services (Other)	28	$82,000
Mining	27	$208,000
Communications and publishing	24	$525,000
Wholesale trade	24	$110,000

FIG. 16 **What are the most common occupational fraud schemes in various industries?**

INDUSTRY	Cases	Billing	Cash larceny	Cash on hand	Check and payment tampering	Corruption	Expense reimbursements	Financial statement fraud	Noncash	Payroll	Register disbursements	Skimming
Banking and financial services	338	11%	14%	23%	12%	36%	7%	8%	11%	2%	3%	9%
Manufacturing	201	27%	8%	15%	12%	51%	18%	10%	28%	5%	3%	7%
Government and public administration	184	15%	11%	11%	9%	50%	11%	5%	22%	7%	2%	11%
Health care	149	26%	7%	13%	13%	36%	16%	11%	19%	17%	1%	12%
Retail	104	20%	10%	19%	9%	28%	8%	12%	34%	5%	13%	13%
Education	96	23%	19%	19%	6%	38%	18%	6%	19%	6%	0%	14%
Insurance	87	20%	9%	3%	18%	45%	8%	7%	11%	3%	1%	11%
Energy	86	20%	2%	10%	12%	53%	10%	3%	27%	7%	2%	10%
Construction	83	37%	12%	8%	19%	42%	23%	16%	23%	14%	1%	13%
Transportation and warehousing	79	25%	8%	8%	9%	46%	15%	8%	28%	3%	3%	13%
Food service and hospitality	75	17%	16%	20%	11%	29%	12%	12%	24%	7%	0%	23%
Technology	62	26%	5%	10%	8%	42%	21%	16%	32%	8%	0%	6%
Religious, charitable, or social services	58	40%	9%	22%	19%	34%	29%	10%	19%	22%	3%	17%
Services (professional)	54	26%	17%	15%	26%	17%	30%	13%	13%	15%	0%	15%
Arts, entertainment, and recreation	50	14%	20%	36%	6%	32%	12%	8%	18%	4%	8%	28%

LESS RISK — MORE RISK

FIG. 17 **What anti-fraud controls are most common?**

Control	Percent of cases	Control in place	Control not in place	Percent reduction
Code of conduct	80%	$110,000	$250,000	56%
Proactive data monitoring/analysis	37%	$ 80,000	$165,000	52%
Surprise audits	37%	$ 75,000	$152,000	51%
External audit of internal controls over financial reporting	67%	$100,000	$200,000	50%
Management review	66%	$100,000	$200,000	50%
Hotline	63%	$100,000	$200,000	50%
Anti-fraud policy	54%	$100,000	$190,000	47%
Internal audit department	73%	$108,000	$200,000	46%
Management certification of financial statements	72%	$109,000	$192,000	43%
Fraud training for employees	53%	$100,000	$169,000	41%
Formal fraud risk assessments	41%	$100,000	$162,000	38%
Employee support programs	54%	$100,000	$160,000	38%
Fraud training for managers/executives	52%	$100,000	$153,000	35%
Dedicated fraud department, function, or team	41%	$100,000	$150,000	33%
External audit of financial statements	80%	$120,000	$170,000	29%
Job rotation/mandatory vacation	19%	$100,000	$130,000	23%
Independent audit committee	61%	$120,000	$150,000	20%
Rewards for whistleblowers	12%	$110,000	$125,000	12%

Control	Percent of cases	Control in place	Control not in place	Percent reduction
Proactive data monitoring/analysis	37%	10 months	24 months	58%
Surprise audits	37%	11 months	24 months	54%
Internal audit department	73%	12 months	24 months	50%
Management certification of financial statements	72%	12 months	24 months	50%
External audit of internal controls over financial reporting	67%	12 months	24 months	50%
Management review	66%	12 months	24 months	50%
Hotline	63%	12 months	24 months	50%
Anti-fraud policy	54%	12 months	24 months	50%
Fraud training for employees	53%	12 months	24 months	50%
Fraud training for managers/executives	52%	12 months	24 months	50%
Formal fraud risk assessments	41%	12 months	24 months	50%
Rewards for whistleblowers	12%	9 months	18 months	50%
Independent audit committee	61%	12 months	23 months	48%
Code of conduct	80%	13 months	24 months	46%
Job rotation/mandatory vacation	19%	10 months	18 months	44%
Dedicated fraud department, function, or team	41%	12 months	20 months	40%
External audit of financial statements	80%	15 months	24 months	38%
Employee support programs	54%	12 months	18 months	33%

FIG. 20 **Was a background check run on the perpetrator prior to hiring?**

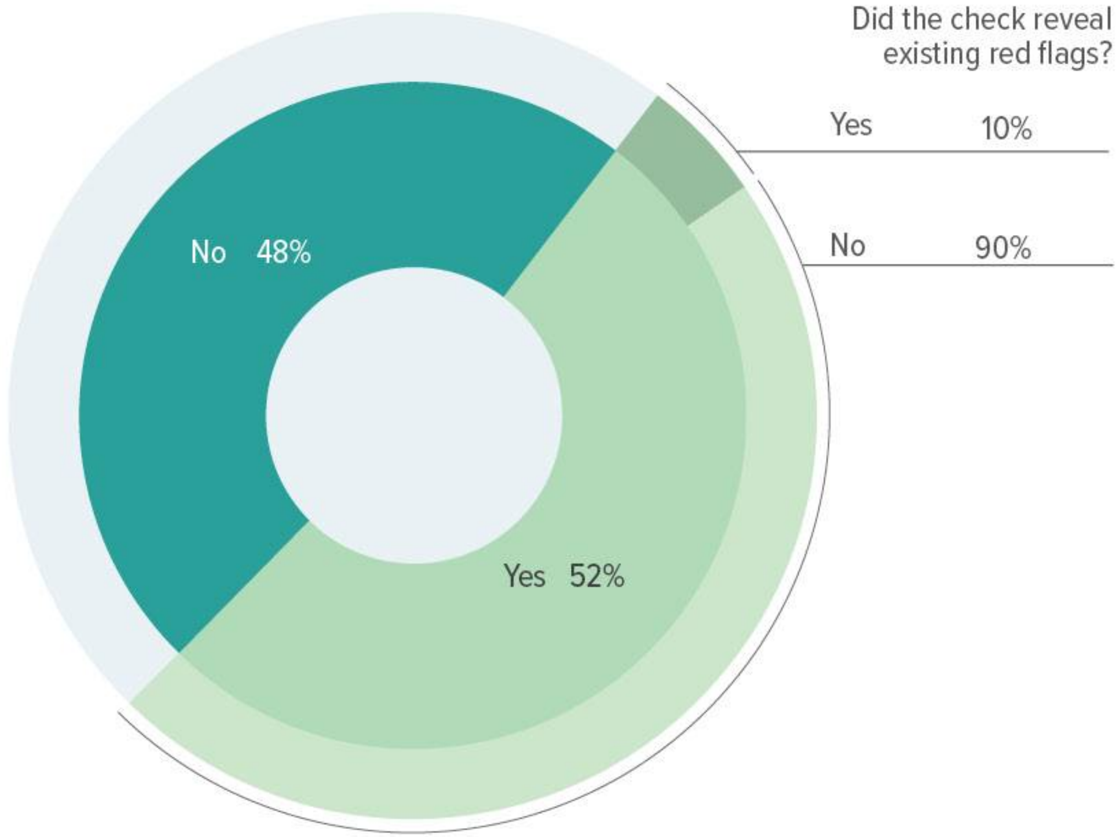


FIG. 21 **What types of background checks were run on the perpetrator prior to hiring?**

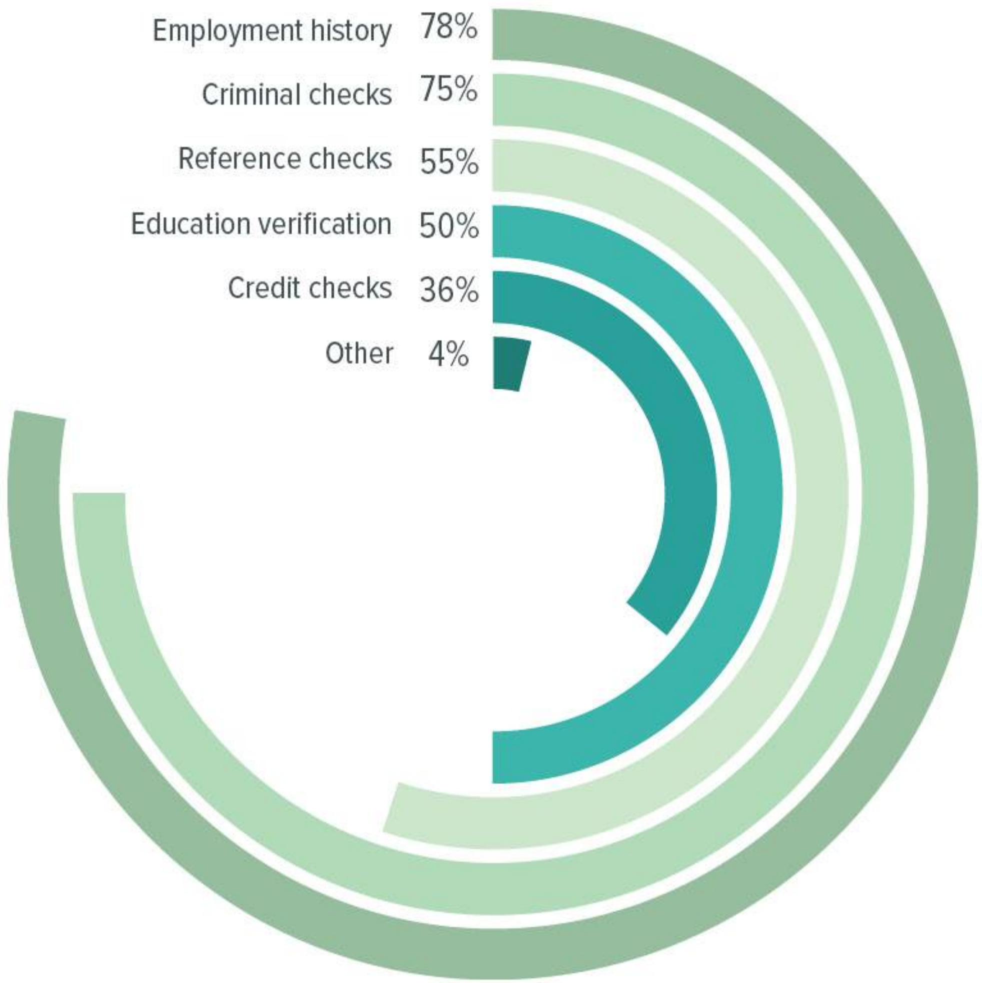
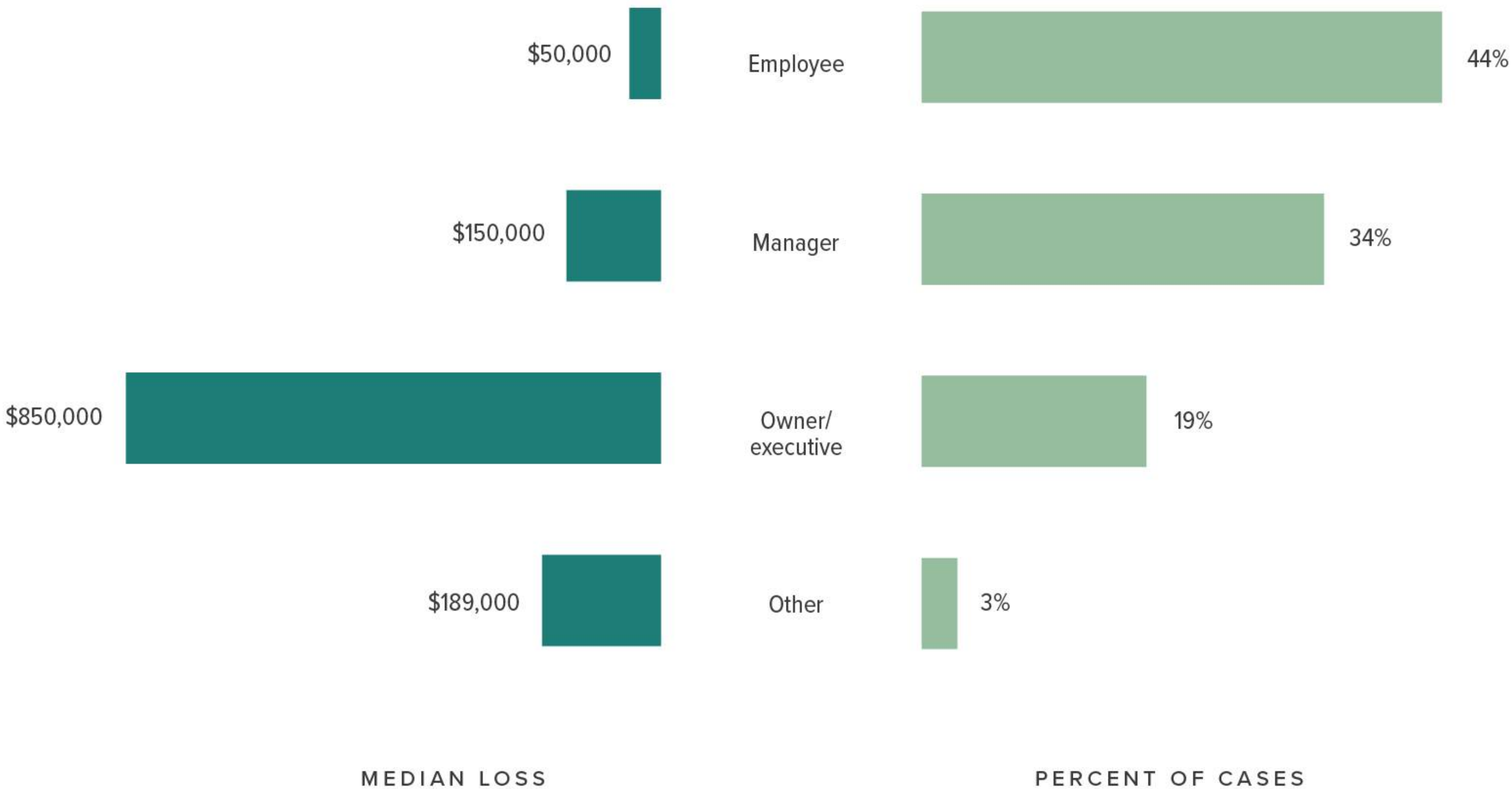


FIG. 24 **How does the perpetrator's level of authority relate to occupational fraud?**



Conclusion

- Insider Threat Vulnerabilities are present in every organization. Control practices are necessary to identify and contain the adverse effects of such threats.

- Thank you for your attention to this presentation.

- **Contact:**
- **Alan E. Small   aesmallcia@verizon.net**