



Occupational Fraud 2022:
A REPORT TO THE NATIONS®





FOREWORD

On behalf of the ACFE and the greater anti-fraud community, I am pleased to present *Occupational Fraud 2022: A Report to the Nations*, the latest exploration by the ACFE into the factors and toll of occupational fraud. While this is our 12th edition of the report, this particular study is unique in that it explores frauds that were investigated largely during a global pandemic—a time when anti-fraud professionals, like so many others, were challenged to find new, innovative ways to conduct much of their work.

And yet, our research shows how successfully Certified Fraud Examiners around the world were able to adapt. Even during this time of disruption, occupational frauds were detected more quickly and losses were limited when compared to prior years. While we always appreciate the participation and dedication of CFEs, this year we are especially grateful for their contributions to this study, which highlights the work they have collectively undertaken during such a challenging time.

Thanks to these anti-fraud experts, our research provides valuable information about the costs, methods, perpetrators, and outcomes of occupational fraud schemes derived from more than 2,000 real cases of fraud affecting organizations in 133 countries and 23 industries. We know that to effectively confront any problem—but certainly one this immense and pervasive—we must first thoroughly understand it. The inaugural *Report to the Nation* was launched in 1996 by ACFE Founder, Dr. Joseph T. Wells, CFE, CPA, because he recognized the need to provide this type of foundational information about occupational fraud. In the decades that followed, we have continued this important line of study to improve our profession's ability to prevent, detect, and respond to fraud.

It is my hope that this report not only honors the CFEs who pushed through the challenges of the pandemic and shared their experiences in investigating fraud during that time, but also provides actionable insight for business leaders, the public, and the anti-fraud community as a whole on how to effectively protect organizations from the harms of occupational fraud.



Bruce Dorris, J.D., CFE, CPA
President and CEO, Association of Certified Fraud Examiners

CONTENTS

Foreword	2	Perpetrator's Education Level	55
Key Findings	4	Collusion by Multiple Perpetrators	56
Introduction	6	Perpetrator's Criminal Background	57
Spotlight: The Global Cost of Fraud	8	Perpetrator's Employment History	57
How Is Occupational Fraud Committed?	9	Behavioral Red Flags Displayed by Perpetrators	58
Categories of Occupational Fraud	9	Human Resources-Related Red Flags	59
Duration of Fraud Schemes	13	Spotlight: Behavioral Red Flags of Fraud	60
Velocity of Fraud Schemes	15	Case Results	62
Spotlight: How Do Perpetrators Conceal Their Frauds?	17	Internal Action Taken Against Perpetrators	62
Spotlight: A Decade of Occupational Fraud	18	Spotlight: Response to Fraud	63
Cryptocurrency Schemes	20	Recovering Fraud Losses	65
Detection	21	Methodology	66
Initial Detection of Occupational Fraud	21	Analysis Methodology	66
Spotlight: Hotline and Reporting Mechanism Effectiveness	24	Survey Participants	67
Reporting Mechanisms	26	Regional Focus	70
Parties to Whom Whistleblowers Report	27	Asia-Pacific	70
Victim Organizations	28	Eastern Europe and Western/Central Asia	72
Type of Organization	28	Latin America and the Caribbean	74
Size of Organization	29	Middle East and North Africa	76
Industry of Organization	32	Southern Asia	78
Anti-Fraud Controls at Victim Organizations	34	Sub-Saharan Africa	80
Spotlight: Modifying Anti-Fraud Controls Following a Fraud	39	United States and Canada	82
Spotlight: COVID's Effect on Occupational Fraud	40	Western Europe	84
Background Checks	41	Statistical Appendix	86
Internal Control Weakness that Contributed to the Fraud	42	Index of Figures	89
Perpetrators	44	Fraud Prevention Checklist	92
Perpetrator's Position	44	Glossary of Terminology	94
Perpetrator's Tenure	46	About the ACFE	95
Perpetrator's Department	46		
Spotlight: How Does Tenure Affect Fraud Risk?	48		
Perpetrator's Gender	51		
Perpetrator's Age	54		

KEY FINDINGS

OUR STUDY COVERED:



CFEs estimate that organizations **LOSE**



MEDIAN LOSS PER CASE:

\$117,000

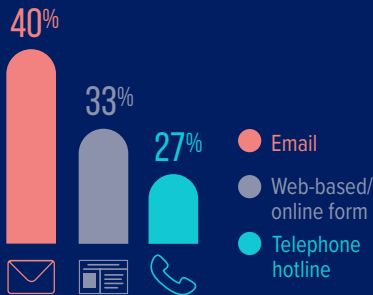
AVERAGE LOSS PER CASE:

\$1,783,000

DETECTION



More than **HALF** of all tips came from employees



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

SCHEMES

ASSET MISAPPROPRIATION SCHEMES are the most common but least costly



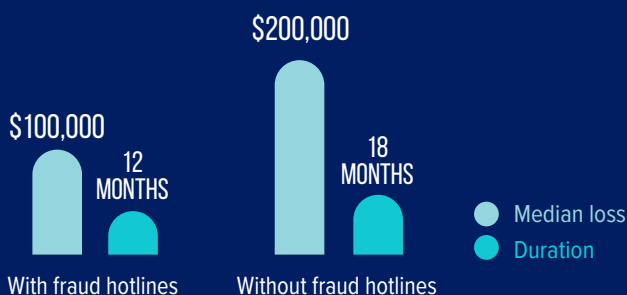
FINANCIAL STATEMENT FRAUD SCHEMES are the least common but most costly



CORRUPTION was the most common scheme in every global region

ORGANIZATIONS WITH HOTLINES

detect fraud more quickly and have lower losses than organizations without hotlines



A TYPICAL FRAUD CASE

causes a loss of **\$8,300** per month

lasts **12 months** before detection

8% of fraud cases involved the use of **CRYPTOCURRENCY**



Among these cases, cryptocurrency was most commonly used for:

48% Making bribery and kickback payments

43% Converting misappropriated assets

KEY FINDINGS

VICTIM ORGANIZATIONS

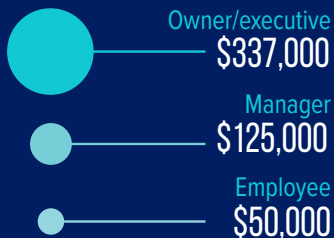
TOP 5 MEDIAN LOSSES BY INDUSTRY



ORGANIZATIONS WITH THE **FEWEST EMPLOYEES** HAD THE HIGHEST MEDIAN LOSS (\$150,000)

PERPETRATORS

Owners/executives committed **only 23%** of occupational frauds, but they caused the largest losses



Nearly **half** of all occupational frauds came from these four departments:



85% of fraudsters displayed **BEHAVIORAL RED FLAGS** of fraud



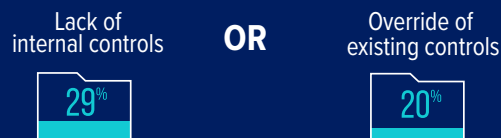
Only 6% of perpetrators had a prior fraud conviction

ANTI-FRAUD CONTROLS

The presence of anti-fraud controls is associated with



Nearly **HALF** of cases occurred due to:



81% of victim organizations **MODIFIED** their anti-fraud controls following the fraud.



CASE RESULTS



61%

of perpetrators were terminated by their employers



58%

of cases were referred to law enforcement



66%

of cases referred to law enforcement resulted in a conviction



50%

of organizations that didn't refer cases to law enforcement cited internal discipline as the reason

INTRODUCTION



This study represents the most comprehensive examination available of the costs, methods, victims, and perpetrators of occupational fraud.

Occupational fraud is very likely the most costly and most common form of financial crime in the world. The term *occupational fraud* refers to frauds that are committed by individuals against the organizations that employ them.¹

There are two key reasons why this type of crime is so prevalent. The first is that any organization with employees must, to some extent, entrust those employees with access to or control over its assets, whether that means keeping its books, managing its bank accounts, safeguarding its inventory, etc. It is this very trust that can make organizations vulnerable to occupational fraud. Because all frauds, at their heart, are based upon breaches of trust. The second reason occupational fraud is so costly and common is simply that there are so many people in a position to commit these crimes. The global labor force consists of more than 3.3 billion people², a large majority of whom will never steal or abuse the trust of their employers. But if even a tiny percentage of these individuals cross the line, the result is millions of occupational fraud schemes being committed annually.

We do not know precisely how many people engage in occupational fraud each year, but we know that the collective harm these criminals inflict is enormous. As you will see in this report, global losses are likely measured in trillions of dollars. This represents money that could have been spent creating jobs, producing goods and services, or providing public services. Instead, it went into the pockets of fraudsters.

The data contained in *Occupational Fraud 2022: A Report to the Nations* represents our best effort to understand and measure the impact of occupational fraud. Based on 2,110 cases of occupational fraud that were investigated between January 2020 and September 2021, we have compiled statistics on the methods used to commit these crimes, the means by which they were detected, the characteristics of both the victims and the perpetrators, and the ways in which victim organizations responded after the frauds were detected.

This report is based on data that was supplied to us by Certified Fraud Examiners (CFEs) throughout the world who took part in the 2021 *Global Fraud Survey*. Each CFE who participated in the study was presented with an online questionnaire consisting of 77 detailed questions about a fraud case the CFE had personally investigated. We are deeply grateful to the CFEs who took part in this survey and shared information so that others could benefit from their experiences. This report is, in many ways, a testament to the dedication and generosity of those CFEs.

The frauds represented in this study were committed in 133 countries, and they targeted organizations in 23 distinct industry categories. They attacked large multinational businesses, small private companies, government agencies, nonprofits, and every other size or type of organization imaginable. This report truly is a global study of occupational fraud, and as its results make clear, no organization is immune from these crimes.

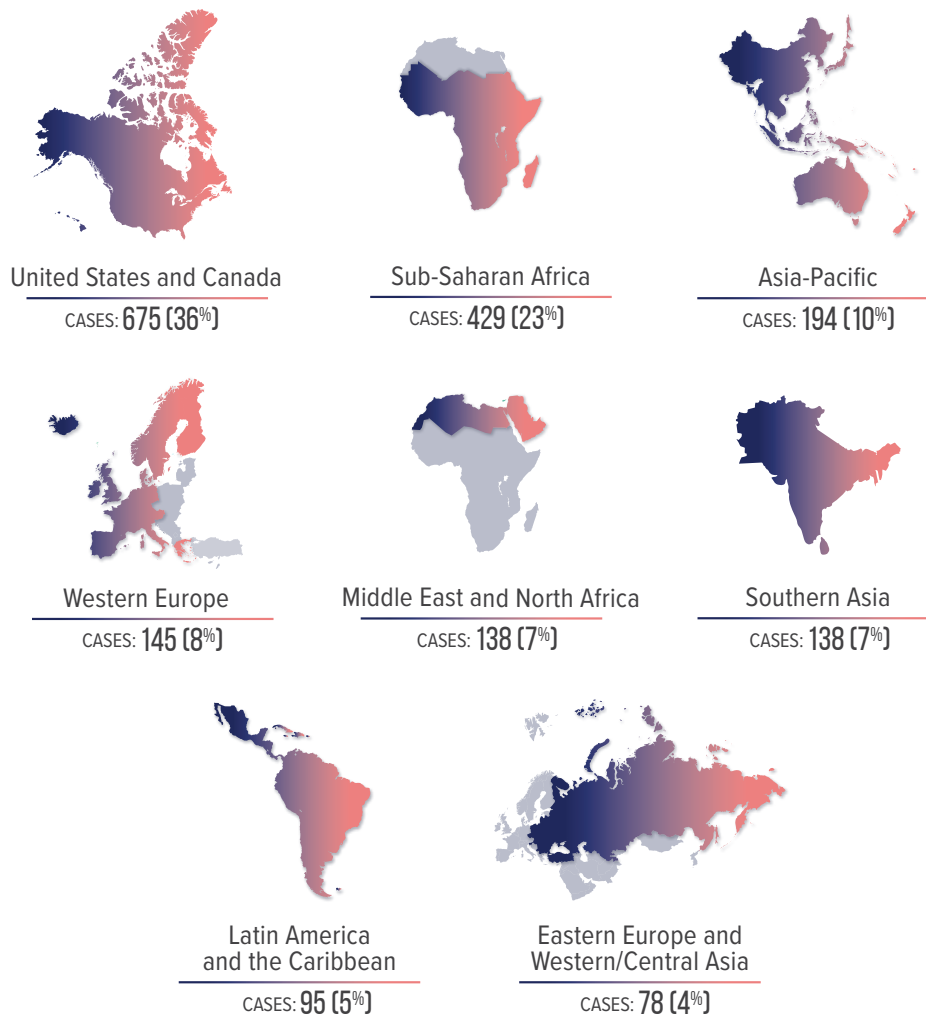
¹ *Occupational fraud* is formally defined as the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.

² The World Bank DataBank, "Labor Force, Total (1990–2020)," <https://data.worldbank.org/indicator/SL.TLF.TOTL.IN>.

THE GOAL OF *OCCUPATIONAL FRAUD 2022: A REPORT TO THE NATIONS* IS TO COMPILE DETAILED INFORMATION ABOUT OCCUPATIONAL FRAUD CASES IN FIVE CRITICAL AREAS:

- The methods by which occupational fraud is committed
- The means by which occupational frauds are detected
- The characteristics of the organizations that are victimized by occupational fraud
- The characteristics of the people who commit occupational fraud
- The results of the cases after the frauds have been detected and the perpetrators identified

FIG. 1 REPORTED CASES BY REGION



THE GLOBAL COST OF FRAUD

Fraud is a truly global problem, affecting organizations in every region and in every industry worldwide. Measuring the true extent of the damage caused by occupational fraud can be challenging due to the inherent nature of concealment and deception involved in most schemes. However, our study provides some valuable insight into the scope of this issue and how it affects organizations everywhere.

OUR STUDY COVERED

2,110 CASES from **133** COUNTRIES

Causing total losses of more than **\$3.6 BILLION**

\$1,783,000
AVERAGE LOSS PER CASE

21% OF CASES HAD LOSSES OF **\$1 MILLION+**

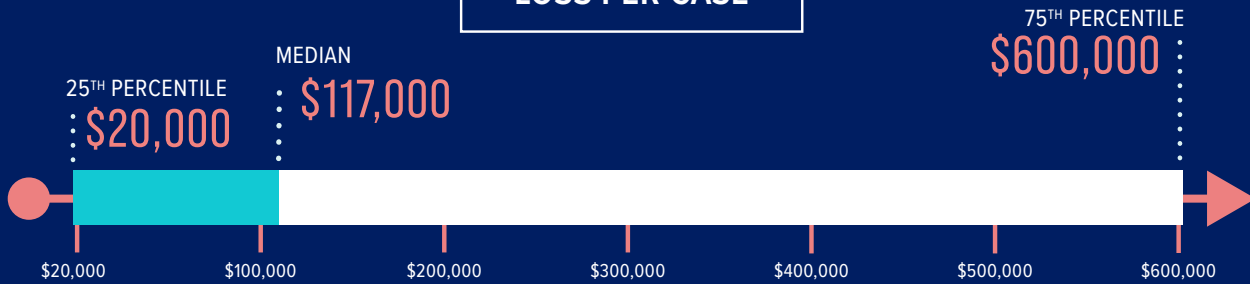
CFEs estimate that organizations **LOSE**

5% of revenue to **FRAUD** each year

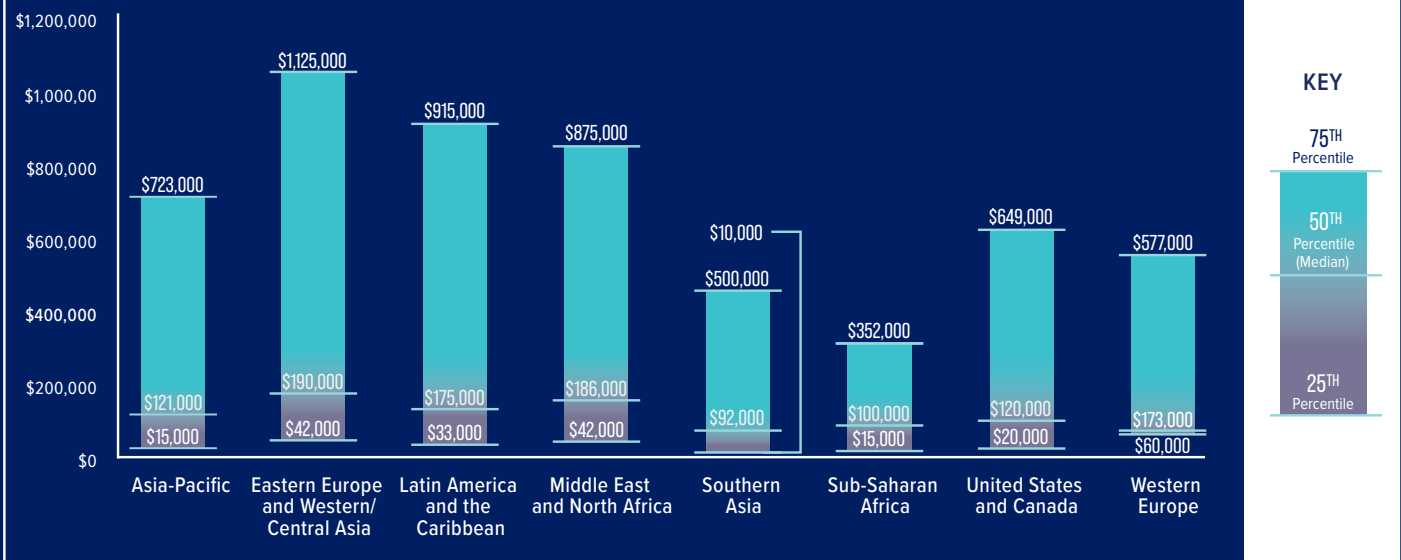
Projected against 2021 GWP (\$94.94 TRILLION), that's more than **\$4.7 TRILLION** lost to **FRAUD GLOBALLY**

WWW.IMF.ORG/EXTERNAL/DATAMAPPER/NGDPD@WEO/WEO WORLD

LOSS PER CASE



LOSS PER REGION



HOW IS OCCUPATIONAL FRAUD COMMITTED?



Since the release of the first *Report to the Nation* in 1996, we have analyzed more than 20,000 cases of occupational fraud reported to us by CFEs. In each study, we have explored the mechanisms used by the fraud perpetrators to defraud their employers. Even with the shift toward digital payments, remote work environments, and technology-based organizations, the schemes and methods fraudsters use to commit occupational fraud remain consistent over time. A taxonomy of these schemes is provided in the *Occupational Fraud and Abuse Classification System*, also commonly referred to as the *Fraud Tree* (see Figure 3).

CATEGORIES OF OCCUPATIONAL FRAUD

At the top level, there are three primary categories of occupational fraud. Asset misappropriation, which involves an employee stealing or misusing the employer's resources, is the most common, with 86% of cases falling under this category. These schemes, however, tend to cause the lowest median loss at USD 100,000 per case (see Figure 2). In contrast, financial statement fraud schemes, in which the perpetrator intentionally causes a material misstatement or omission in the organization's financial statements, are the least common (9% of schemes) but costliest (USD 593,000) category. The third category, corruption—which includes offenses such as bribery, conflicts of interest, and extortion—falls in the middle in terms of both frequency and losses. These schemes occur in 50% of cases and cause a median loss of USD 150,000.

FIG. 2 HOW IS OCCUPATIONAL FRAUD COMMITTED?

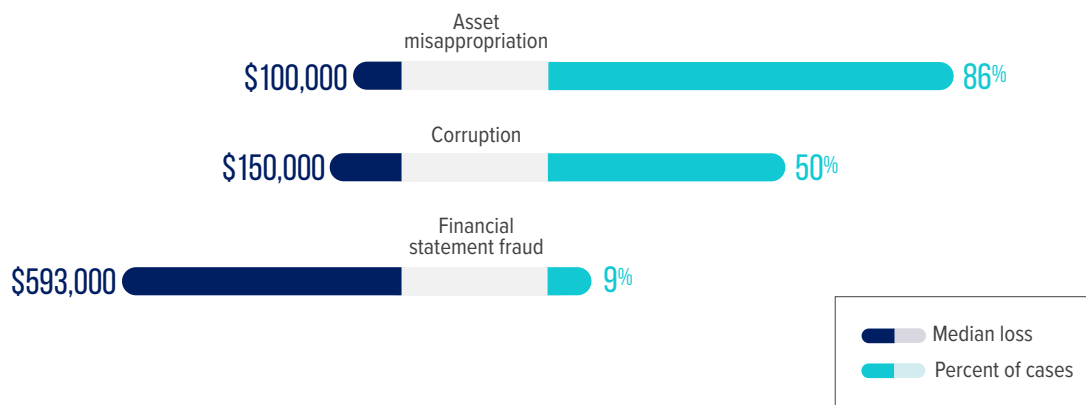
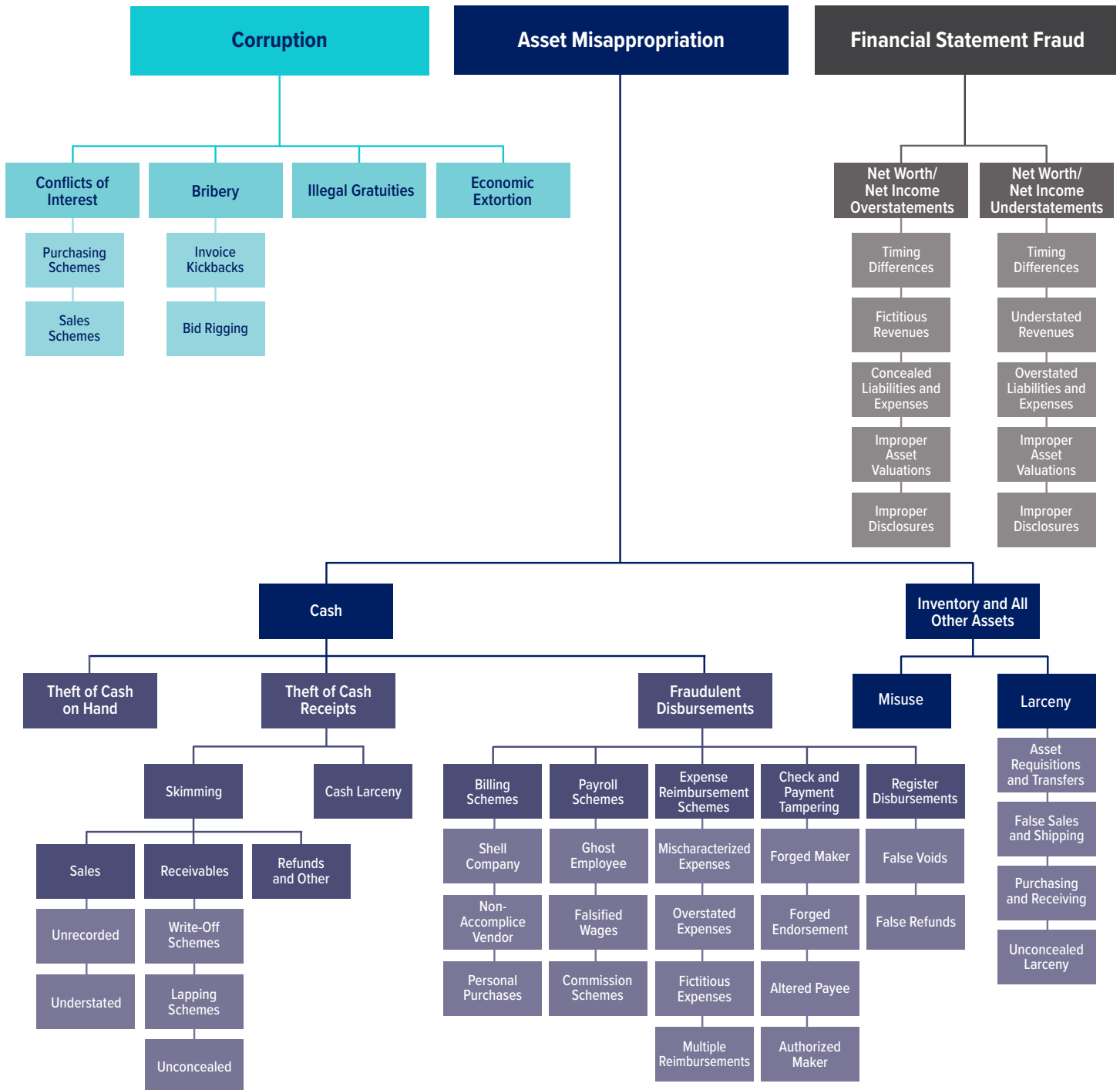


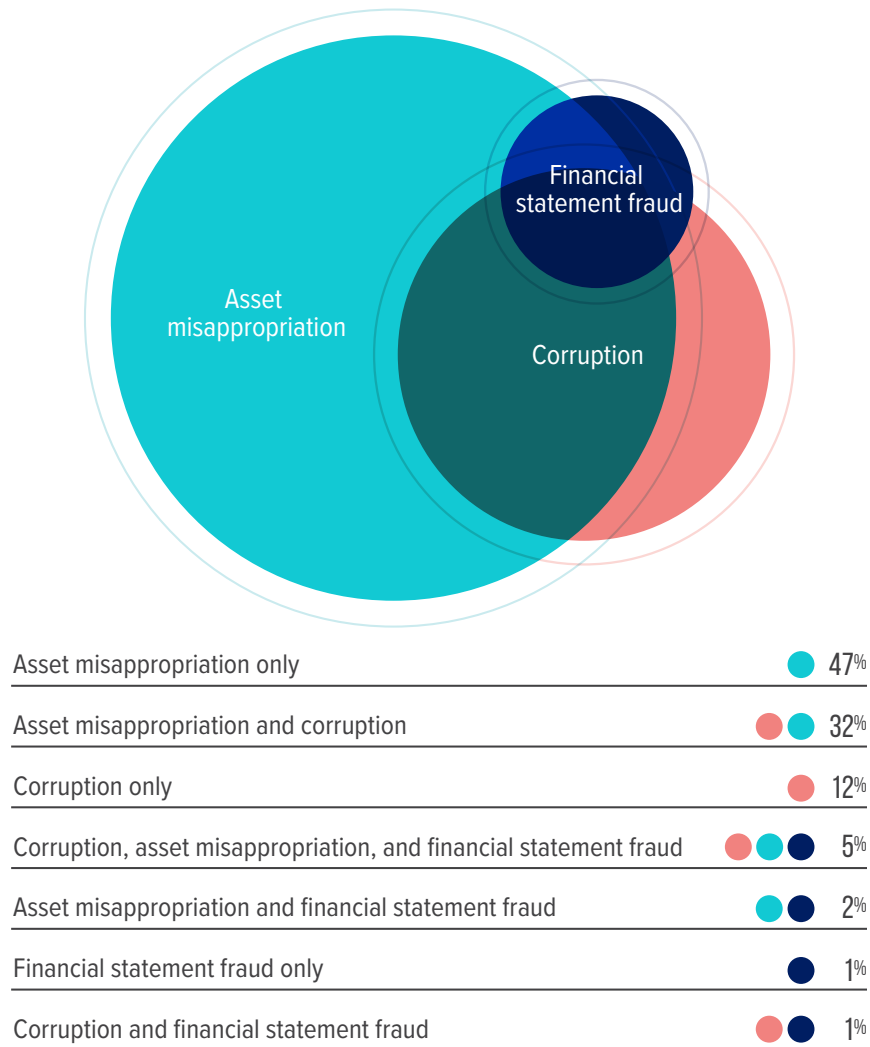
FIG. 3 OCCUPATIONAL FRAUD AND ABUSE CLASSIFICATION SYSTEM (THE FRAUD TREE)³



³ The definitions for many of the categories of fraud schemes in the Fraud Tree are found in the Glossary of Terminology on page 94.

Fraudsters do not necessarily limit themselves to one method of stealing. Of the cases in our study, 40% involved more than one of the three primary categories of occupational fraud. As noted in Figure 4, 32% of fraudsters committed both asset misappropriation and corruption schemes as part of their crime, 2% misappropriated assets and committed financial statement fraud, 1% engaged in both corruption and financial statement fraud, and 5% included all three categories in their schemes.

FIG. 4 HOW OFTEN DO FRAUDSTERS COMMIT MORE THAN ONE TYPE OF OCCUPATIONAL FRAUD?



ASSET MISAPPROPRIATION SCHEMES
are the most common but least costly

86%
of cases

\$100,000
median loss

FINANCIAL STATEMENT FRAUD SCHEMES
are the least common but most costly

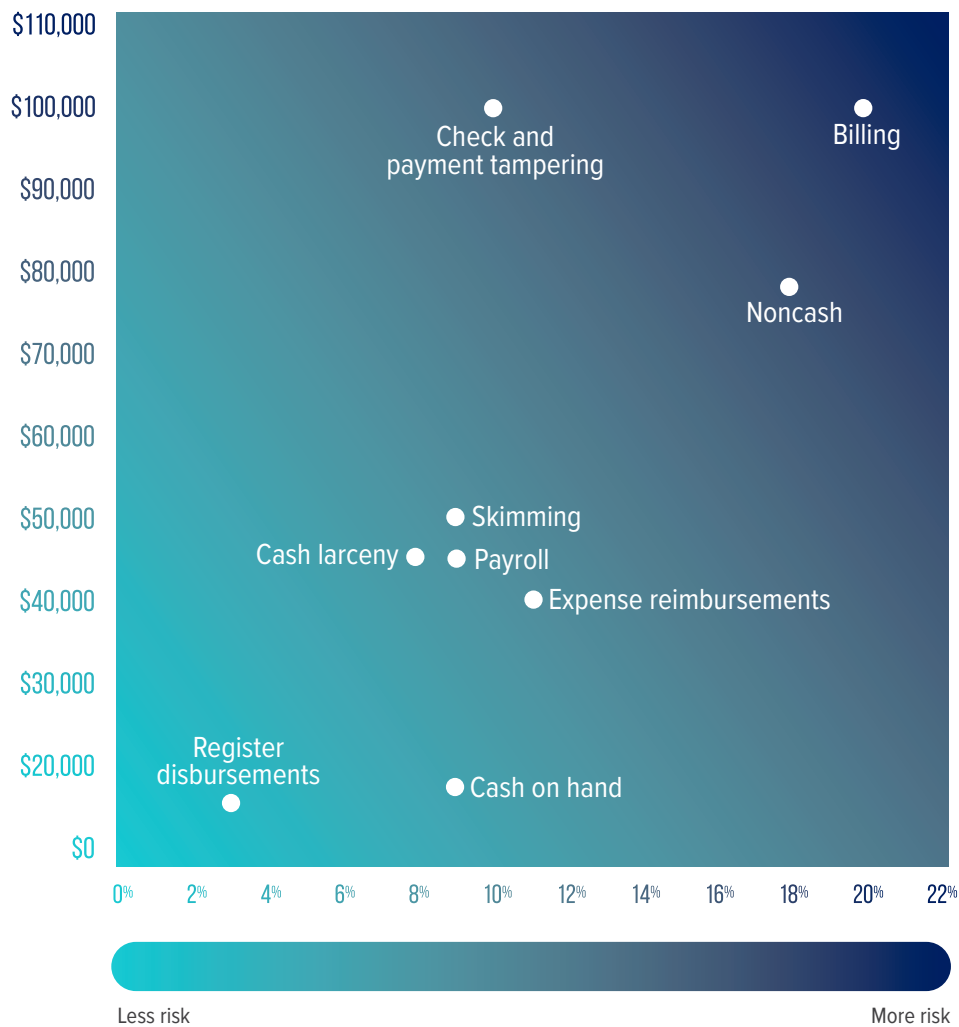
9%
of cases

\$593,000
median loss

ASSET MISAPPROPRIATION SUB-SCHEMES

Because asset misappropriations make up such a large percentage of occupational fraud cases, we divide these frauds into nine distinct categories to better illustrate how they affect organizations. Figure 5 is a heat map that shows the frequency and median loss of each asset misappropriation sub-scheme (see Glossary on page 94 for definitions of each sub-scheme). Billing schemes present a significant risk given that they are the most common form of asset misappropriation and also cause the highest median loss. Other high risks based on the combination of frequency and financial impact are check and payment tampering, as well as noncash schemes (such as theft of physical assets, investments, or proprietary information).

FIG. 5 WHICH ASSET MISAPPROPRIATION SCHEMES PRESENT THE GREATEST RISK?

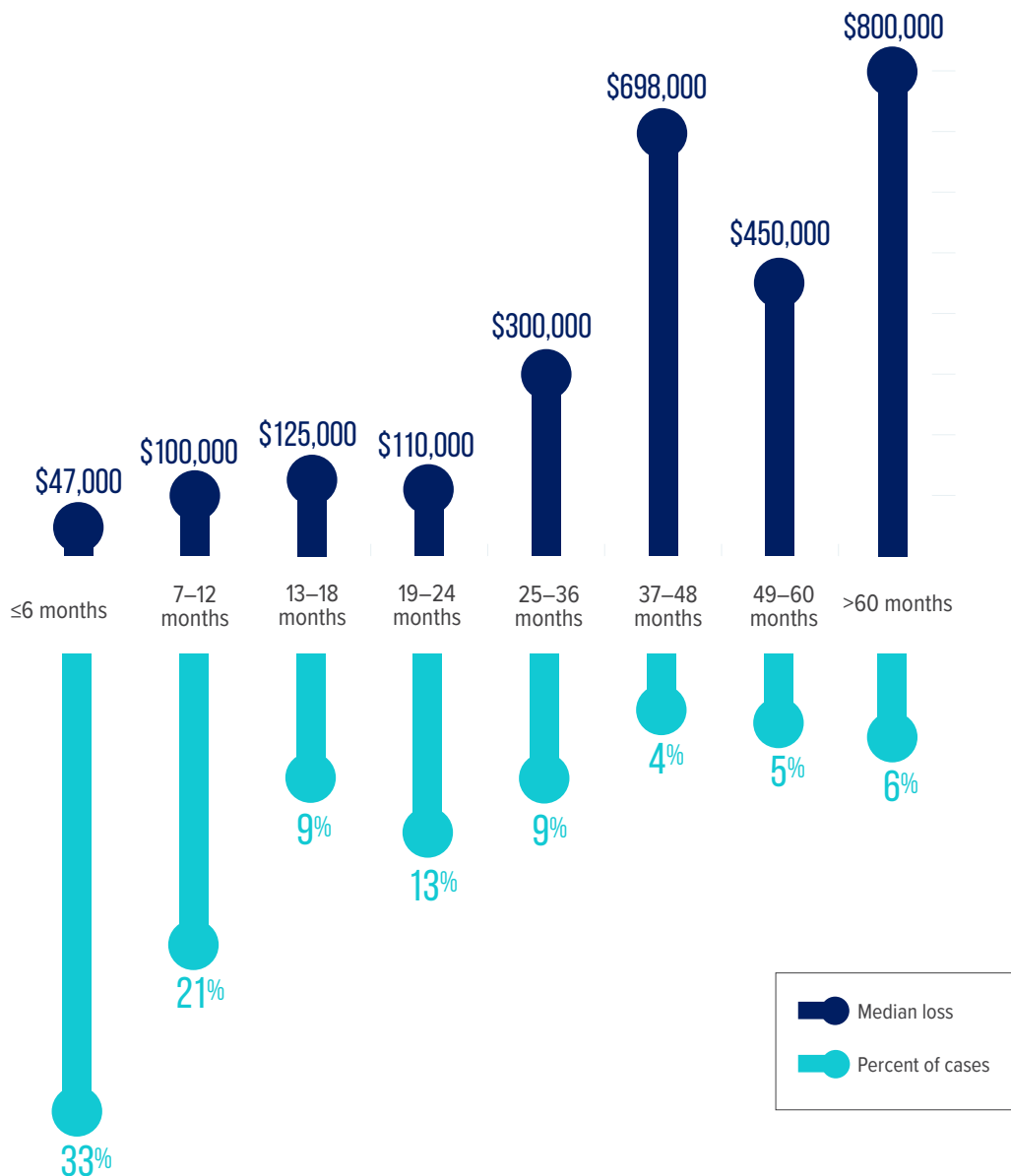


Category	Number of cases	Percent of all cases	Median loss
Billing	416	20%	\$100,000
Noncash	385	18%	\$78,000
Expense reimbursements	232	11%	\$40,000
Check and payment tampering	208	10%	\$100,000
Cash on hand	199	9%	\$15,000
Skimming	198	9%	\$50,000
Payroll	198	9%	\$45,000
Cash larceny	169	8%	\$45,000
Register disbursements	58	3%	\$10,000

DURATION OF FRAUD SCHEMES

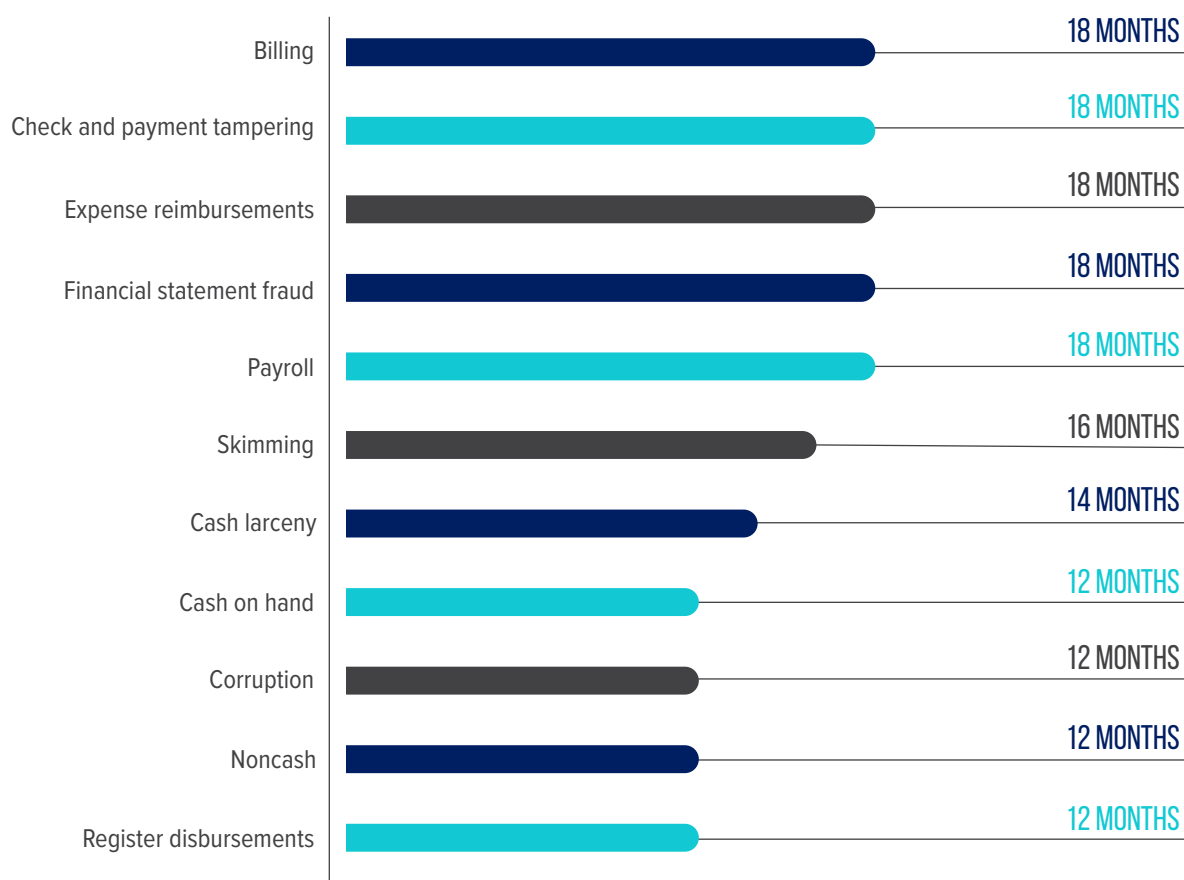
Try as they might, organizations cannot prevent all fraud; if an organization is operational long enough, eventually an employee will commit fraud. Consequently, the ability to quickly detect fraud is crucial. Our research indicates that the median duration of fraud—that is, the typical time between when a fraud begins and when it is detected—is 12 months. Additionally, Figure 6 shows that the longer a fraud remains undetected, the greater the financial loss.

FIG. 6 HOW DOES THE DURATION OF A FRAUD RELATE TO MEDIAN LOSS?



When designing anti-fraud controls, assessing fraud risks, and implementing proactive detection measures, it is helpful to understand the potential impact of different types of fraud schemes. In addition to analyzing the frequency and median loss of the categories of occupational fraud (see Figures 2 and 5), we also examined the duration of cases (in months) in each category. As noted in Figure 7, companies tend to catch register disbursements, noncash, corruption, and cash on hand schemes the quickest (12 months). Other schemes such as billing, check and payment tampering, expense reimbursements, financial statement fraud, and payroll typically last a year and a half before being uncovered. Skimming and cash larceny typically last 16 and 14 months, respectively.

FIG. 7 HOW LONG DO DIFFERENT OCCUPATIONAL FRAUD SCHEMES LAST?

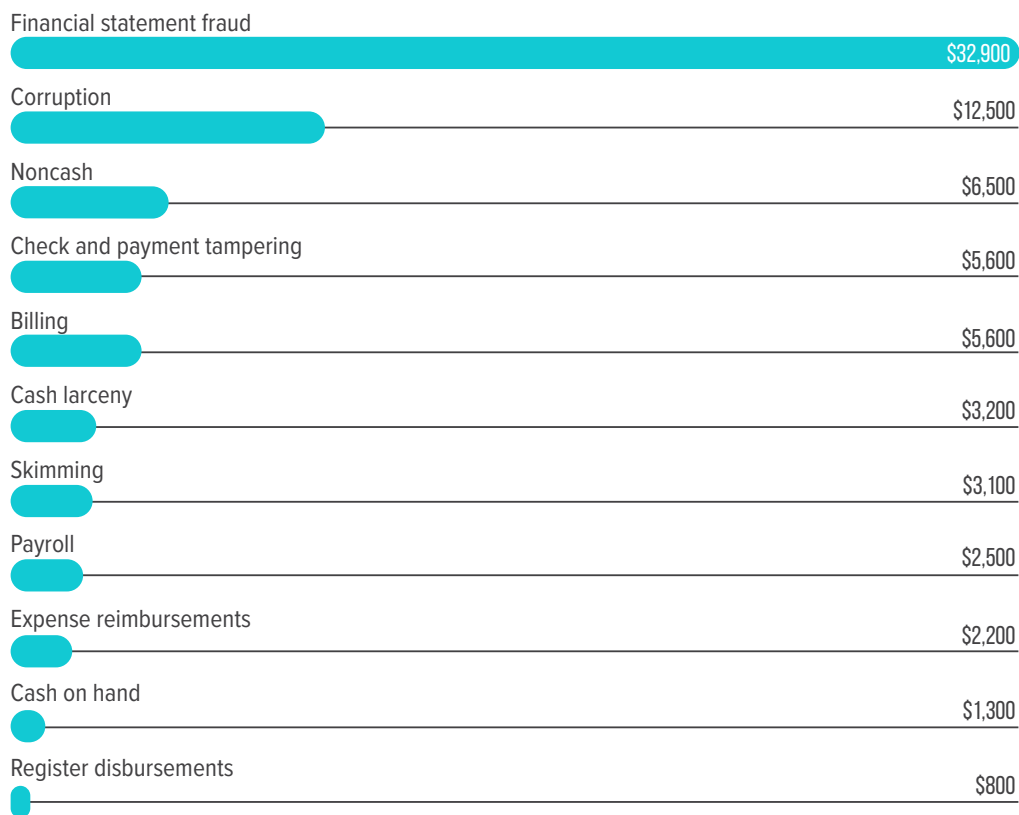


VELOCITY OF FRAUD SCHEMES

Fraud schemes affect companies differently, and organizations must make decisions about how and where to direct their anti-fraud efforts. Therefore, we analyzed how quickly occupational fraud tends to cause harm, as well as the variation in this speed among different scheme types.

To determine the velocity for different types of fraud, we divided the loss amount by the number of months the scheme lasted before detection. The median velocity for all cases reported was a loss of USD 8,300 per month. Analyzing the velocity by scheme type, however, reveals that certain types of occupational fraud cause damage much faster than others. As Figure 8 shows, financial statement fraud schemes have the greatest velocity of USD 32,900 per month, followed by corruption schemes, with a velocity of USD 12,500 per month. Organizations can use this data to prioritize their resources—for example, by investing more in measures aimed at protecting against high-velocity schemes.

FIG. 8 WHAT IS THE TYPICAL VELOCITY (MEDIAN LOSS PER MONTH) OF DIFFERENT OCCUPATIONAL FRAUD SCHEMES?



Our analysis also reveals differences in scheme velocity based on the number of perpetrators involved in a case, as well as what position the primary perpetrator holds. Schemes with three or more perpetrators escalate faster than those with just one or two perpetrators. Likewise, schemes committed by an owner/executive have a velocity nearly three times that of schemes committed by employees and manager-level individuals. These findings emphasize how those in the highest positions can damage the company much more quickly than those in lower-level positions.

	Median loss	Median duration	Scheme velocity (loss per month)
One perpetrator	\$57,000	12 months	\$4,800
Two perpetrators	\$145,000	12 months	\$12,100
Three or more perpetrators	\$219,000	12 months	\$18,300
Employee	\$50,000	8 months	\$6,300
Manager	\$125,000	16 months	\$7,800
Owner/executive	\$337,000	18 months	\$18,700
<100 employees	\$150,000	16 months	\$9,400
100+ employees	\$100,000	12 months	\$8,300

A TYPICAL FRAUD CASE



causes a loss of **\$8,300** per month



lasts **12 months** before detection

HOW DO PERPETRATORS CONCEAL THEIR FRAUDS?

Examining the methods fraudsters use to conceal their crimes can assist organizations in more effectively detecting and preventing similar schemes moving forward.

TOP 5 CONCEALMENT METHODS USED BY FRAUDSTERS



39%

Created fraudulent physical documents



32%

Altered physical documents



28%

Created fraudulent electronic documents or files



25%

Altered electronic documents or files



23%

Destroyed or withheld physical documents



12% of cases did not involve any attempts to conceal the fraud

EVIDENCE



57%

OF CASES involved the creation of fraudulent evidence

Created fraudulent evidence



Altered existing evidence



Deleted or destroyed evidence



38%

OF CASES involved concealment methods affecting BOTH physical and electronic evidence.

Both physical and electronic evidence



Electronic evidence



Physical evidence



CONCEALMENT BY POSITION



48%

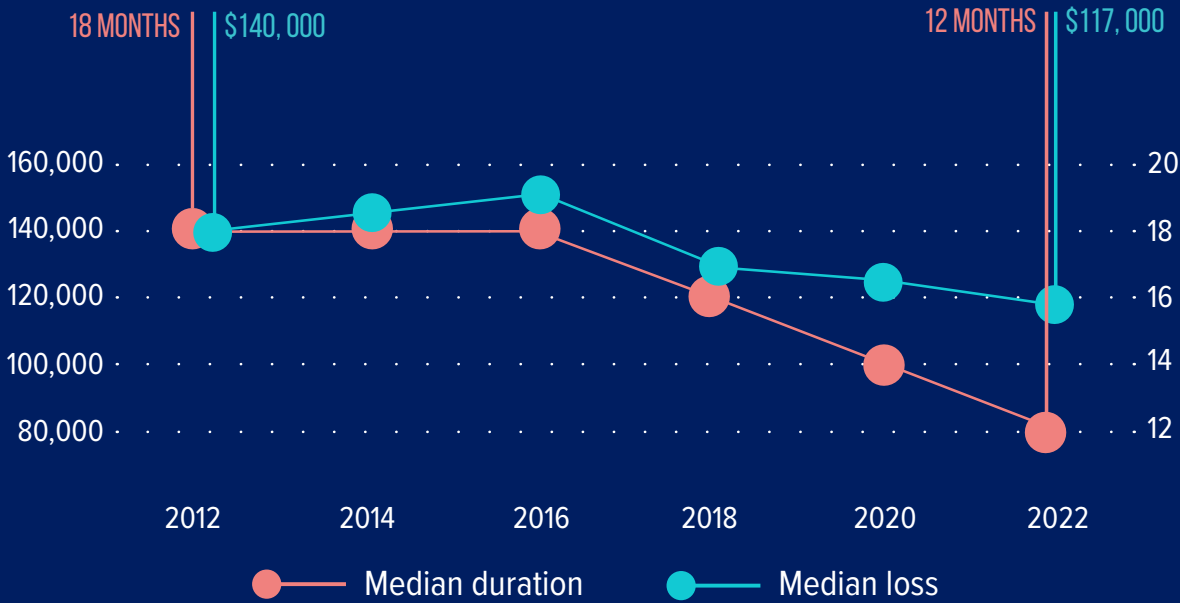
of executive-level perpetrators **DESTROYED** evidence.



61%

of managers **CREATED** fraudulent evidence.

A DECADE OF OCCUPATIONAL FRAUD: TRENDS FROM 2012-2022



Frauds are being caught **FASTER** and causing **SMALLER** losses.

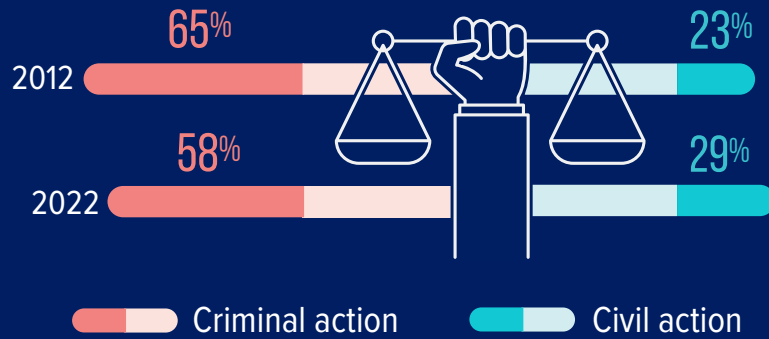
Median losses down

↓16%

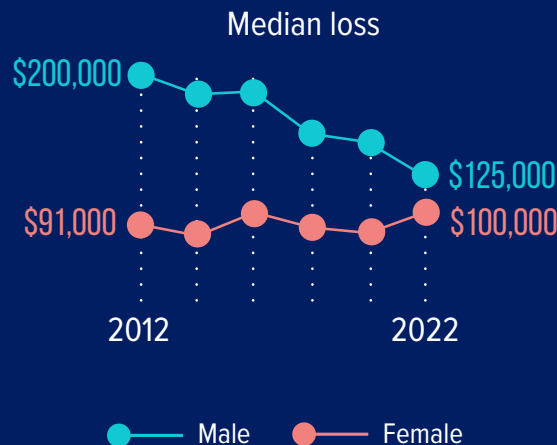
Median duration down

↓33%

Fewer organizations are pursuing **CRIMINAL PROSECUTION**, but more are taking **CIVIL ACTION** against the perpetrator.



MEN are perpetrating an **INCREASING** percentage of **FRAUDS**, but the gap in **LOSSES** has **NARROWED**.



65% ↑ 73%
2012 2022

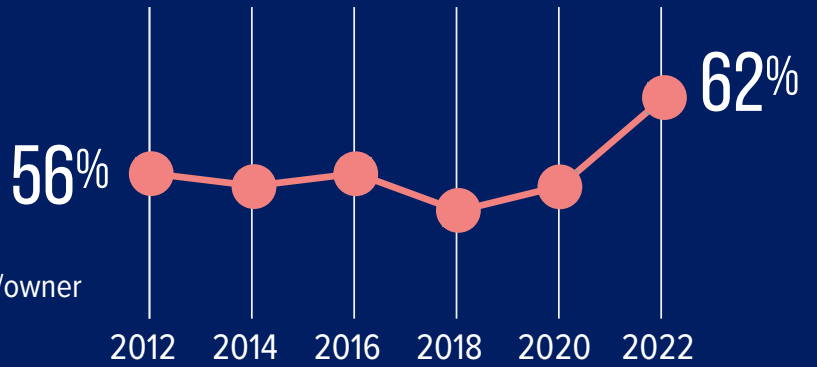


35% ↓ 27%
2012 2022

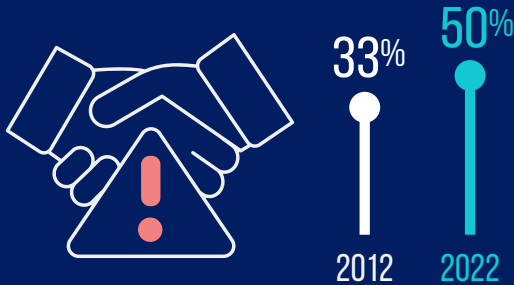
More perpetrators are in roles with **HIGHER LEVELS OF AUTHORITY**



Manager/executive/owner



The percentage of cases involving **CORRUPTION** is on the **RISE**



FRAUDSTERS are **COLLABORATING MORE**



1 Perpetrator



2+ Perpetrators



Implementation rates for 17 of the 18 analyzed anti-fraud controls have

INCREASED OVER THE LAST DECADE



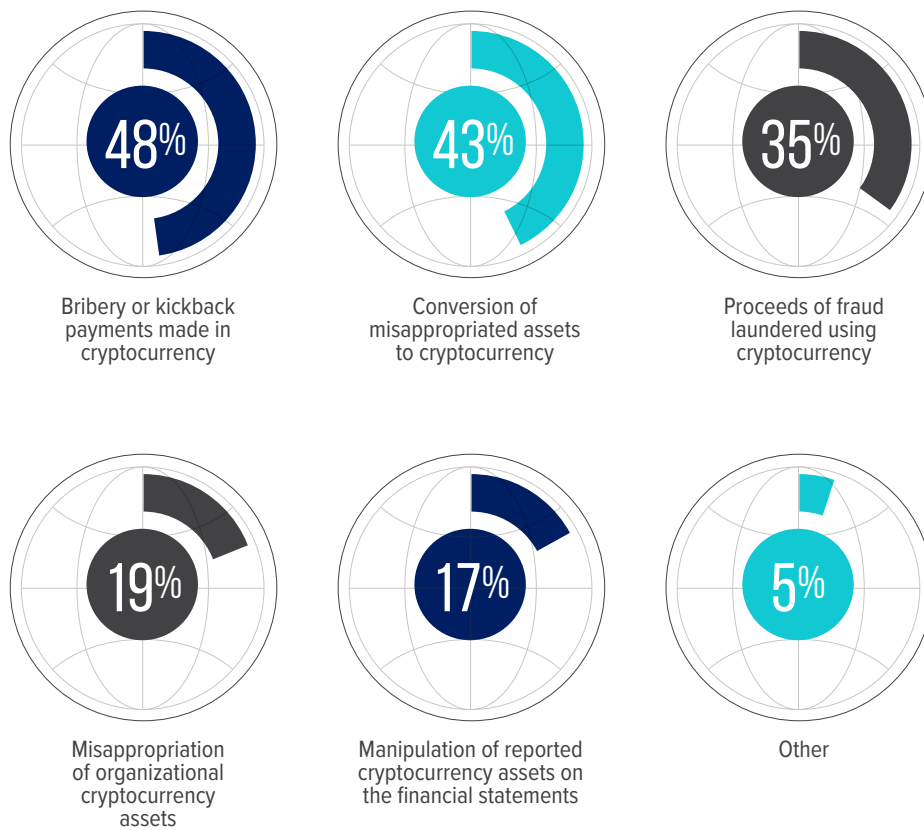
These five have **INCREASED** the most:

	2012	2022	Increase
Hotline	54%	70%	16%
Fraud training for employees	47%	61%	14%
Anti-fraud policy	47%	60%	13%
Fraud training for managers/executives	47%	59%	12%
Formal fraud risk assessments	36%	46%	11%

CRYPTOCURRENCY SCHEMES

The rise of blockchain technology, along with more organizations incorporating the use of cryptocurrency into their regular operations, creates another opportunity for individuals to perpetrate fraud. Only 8% of the frauds in our study involved the use of cryptocurrency (though anecdotal evidence suggests this number will rise in future years). Among these cases, the most common ways cryptocurrency was utilized were making bribery and kickback payments in cryptocurrency (48%) or converting misappropriated assets to cryptocurrency (43%).

FIG. 9 AMONG FRAUDS INVOLVING CRYPTOCURRENCY, HOW WAS IT USED?



8% of fraud cases involved **THE USE OF CRYPTOCURRENCY**

Among these cases, cryptocurrency was most commonly used for:



DETECTION



Detection is an essential step in fraud investigation because the speed with which fraud is detected—as well as the way it is detected—can have a substantial impact on the magnitude of the fraud. It is also an important component of fraud prevention because fraud examiners can take steps to improve how they detect fraud within their organizations. As a result, this might increase staff’s perception that fraud will be detected and possibly deter future misconduct. Our data explores how fraud is initially detected, when it is detected, and who reports it.



INITIAL DETECTION OF OCCUPATIONAL FRAUD AND TIP SOURCES

Knowing the most common methods by which fraud is discovered is the foundation for effective detection of occupational fraud. Despite the increasing number of advanced fraud detection techniques available to organizations, tips were still the most common way occupational frauds were discovered in our study by a wide margin, as they have been in every one of our previous reports. As shown in Figure 10, 42% of cases in our study were uncovered by tips, which is nearly three times as many cases as the next most common detection method. Therefore, implementing effective processes to solicit and thoroughly evaluate tips is a crucial priority for fraud examiners.

Figure 11 identifies the sources of tips that led to fraud detection. More than half of all tips came from employees, while nearly a third of tips came from outside parties, including customers, vendors, and competitors. This reinforces the fact that anti-fraud education and the communication of designated reporting mechanisms should target both internal staff and external parties.

FIG. 10 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED?

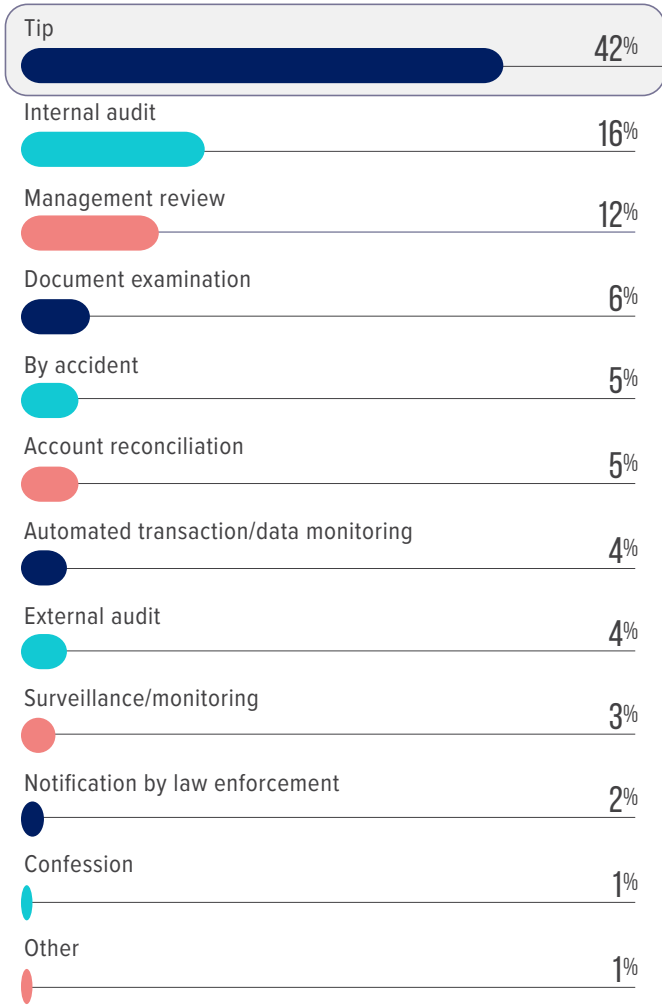
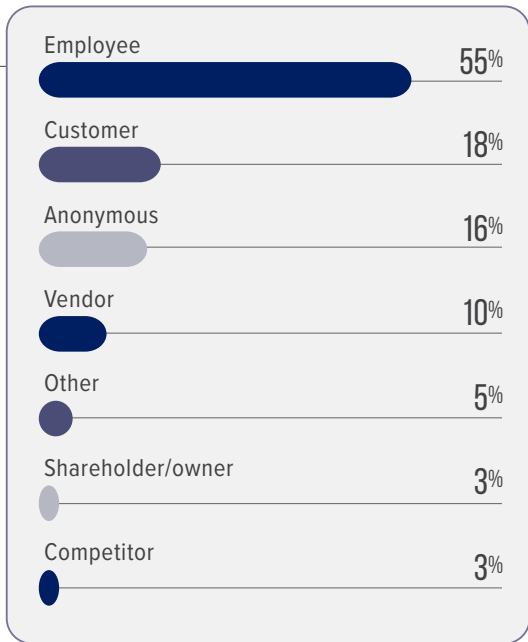


FIG. 11 WHO REPORTS OCCUPATIONAL FRAUD?

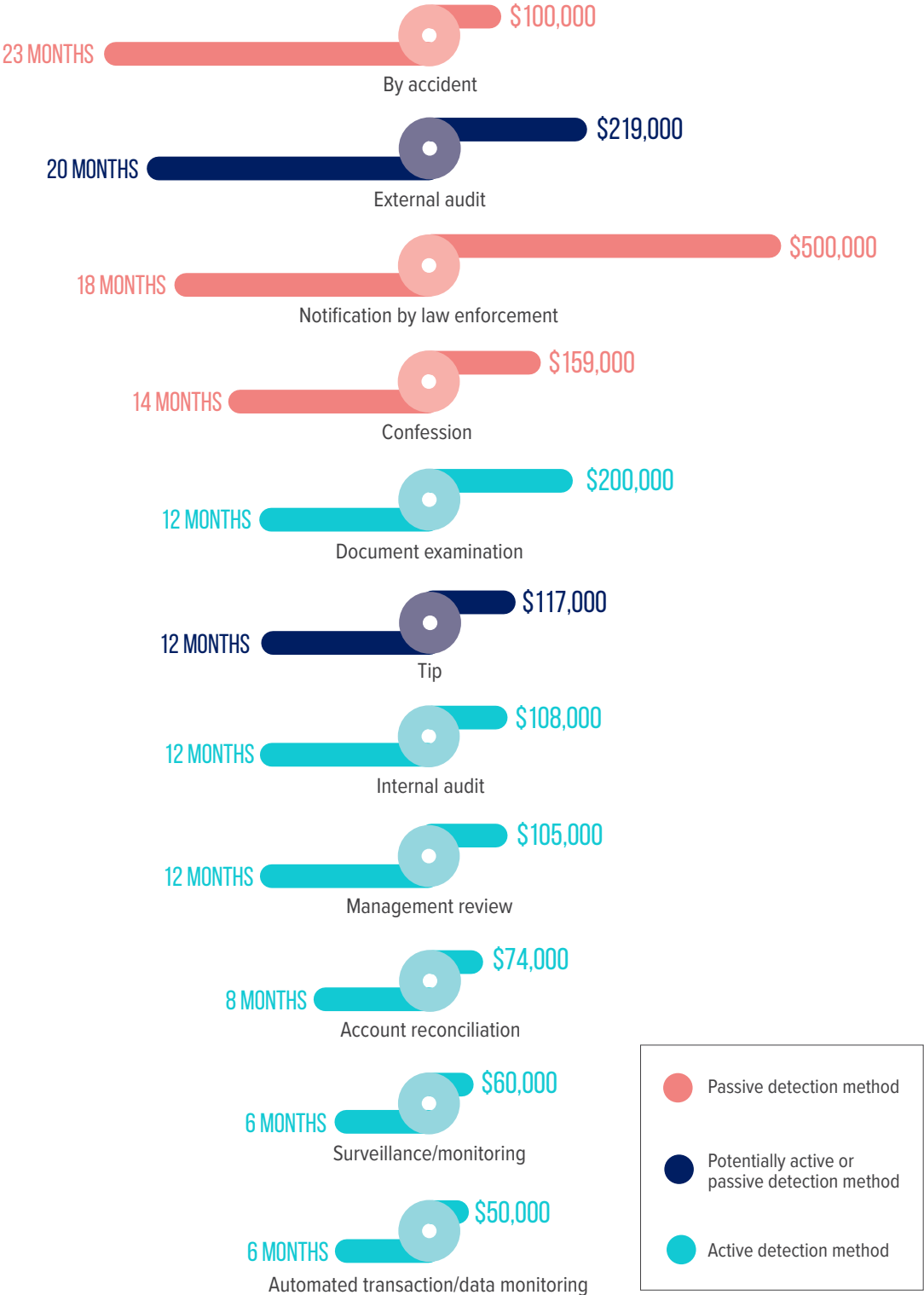


MEDIAN LOSS AND DURATION BY DETECTION METHOD

Results from our data show that some fraud detection methods are more effective than others in that they correlate to lower fraud losses. Figure 12 shows the relationship between the detection method and the associated fraud scheme duration and loss, respectively. In this chart, the pink bars indicate schemes that were detected by passive methods—that is, the fraud came to the victim’s attention through no effort of their own—including notification by police, by accident, or by a fraudster’s confession. In general, most passively detected schemes lasted longer and were associated with higher median losses relative to all other detection methods. The light blue bars indicate active detection methods—those that involved a process or effort designed (at least in part) to proactively detect fraud—such as document examination or surveillance/monitoring. Schemes discovered through an active method were shorter in duration and had lower median losses than those detected passively. The dark blue bars indicate detection methods that could potentially be passive or active, including tips and external audit.

This data highlights that when fraud is detected proactively, it tends to be detected more quickly and results in lower losses; in contrast, passive detection results in longer-lasting schemes and increased financial damage to the victim. Anti-fraud controls such as automated transaction/data monitoring, surveillance, account reconciliation, ongoing and proactive management review, and internal audit departments are all tools that can lead to more effective detection of occupational fraud.

FIG. 12 HOW DOES DETECTION METHOD RELATE TO FRAUD LOSS AND DURATION?

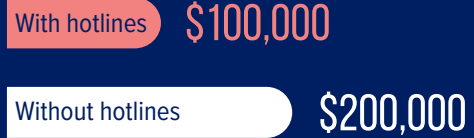


HOTLINE AND REPORTING MECHANISM EFFECTIVENESS

Maintaining a hotline or reporting mechanism increases the chances of earlier fraud detection and reduces losses. Fraud awareness training encourages tips through reporting mechanisms.

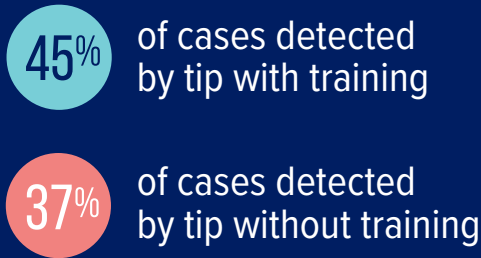
70% of **VICTIM ORGANIZATIONS** had hotlines

Fraud losses were **2X HIGHER** at organizations without hotlines



EFFECT OF EMPLOYEE AND MANAGER FRAUD AWARENESS TRAINING ON HOTLINES AND REPORTING

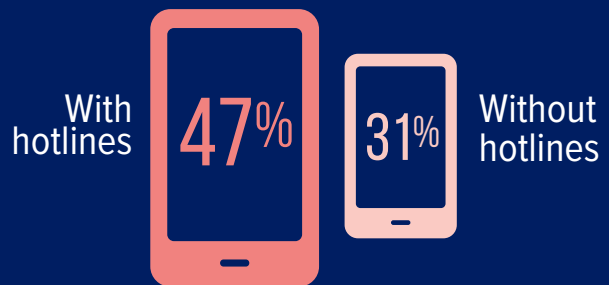
TRAINING INCREASES the likelihood of detection by tip



Reports of fraud are **MORE LIKELY TO BE SUBMITTED** through hotlines with training



Organizations with hotlines are more likely to detect fraud **BY TIP**

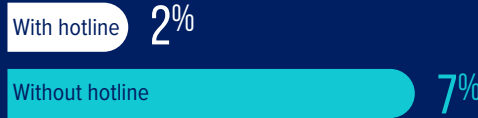


Percent of cases detected by tip

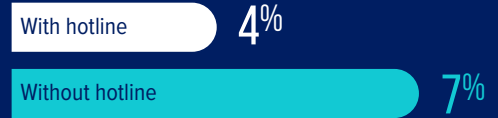
ORGANIZATIONS WITHOUT HOTLINES ARE 3.5X MORE LIKELY to discover fraud through an external audit and nearly 2X more likely by accident



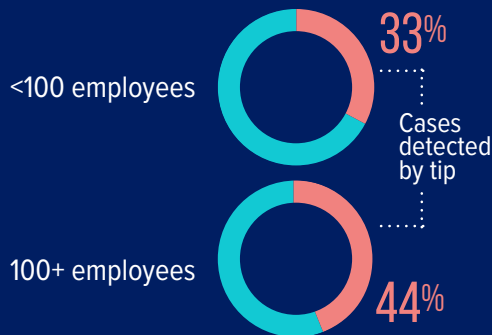
External audit



By accident



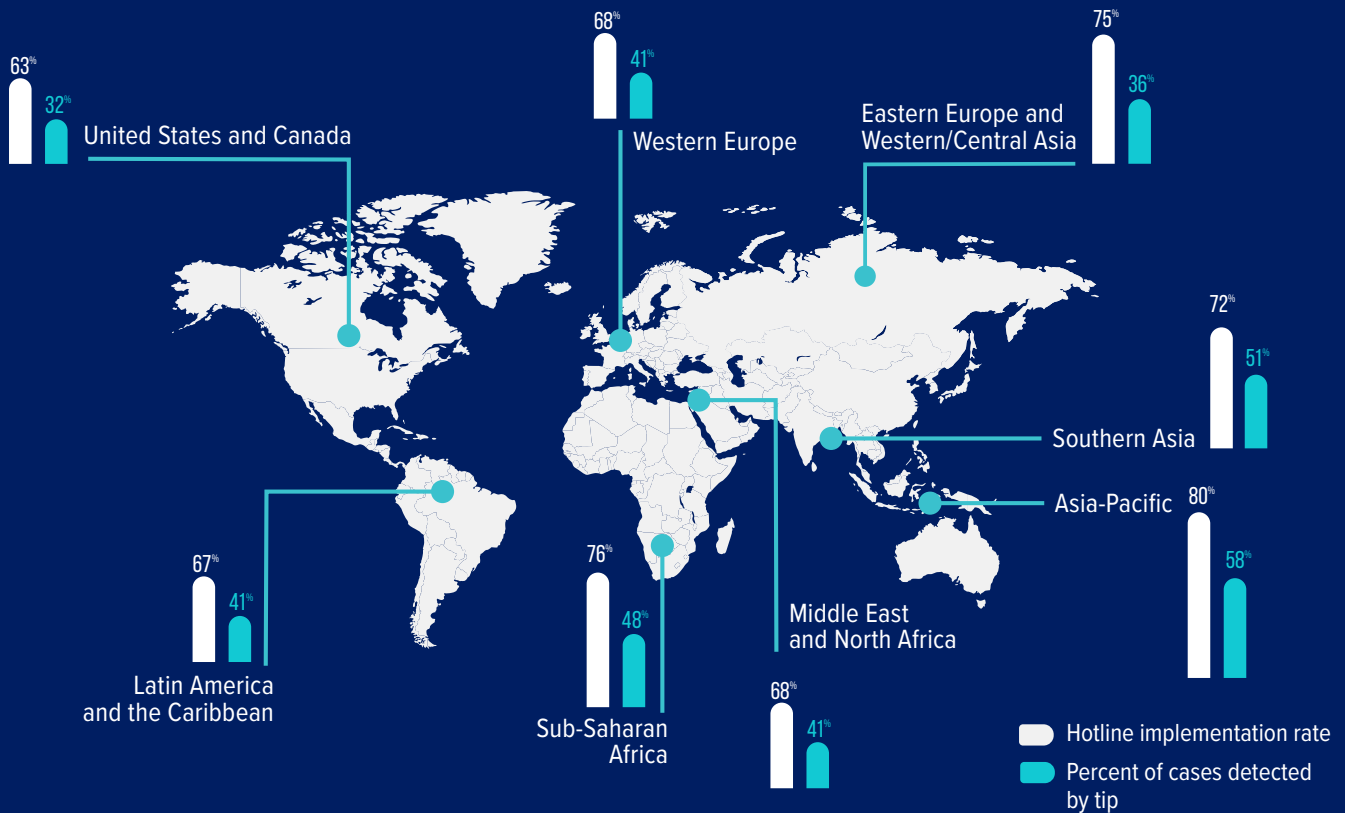
LARGE ORGANIZATIONS are especially likely to detect occupational fraud by tip



Since 2012, the percent of tips made through hotlines has **INCREASED DRAMATICALLY**



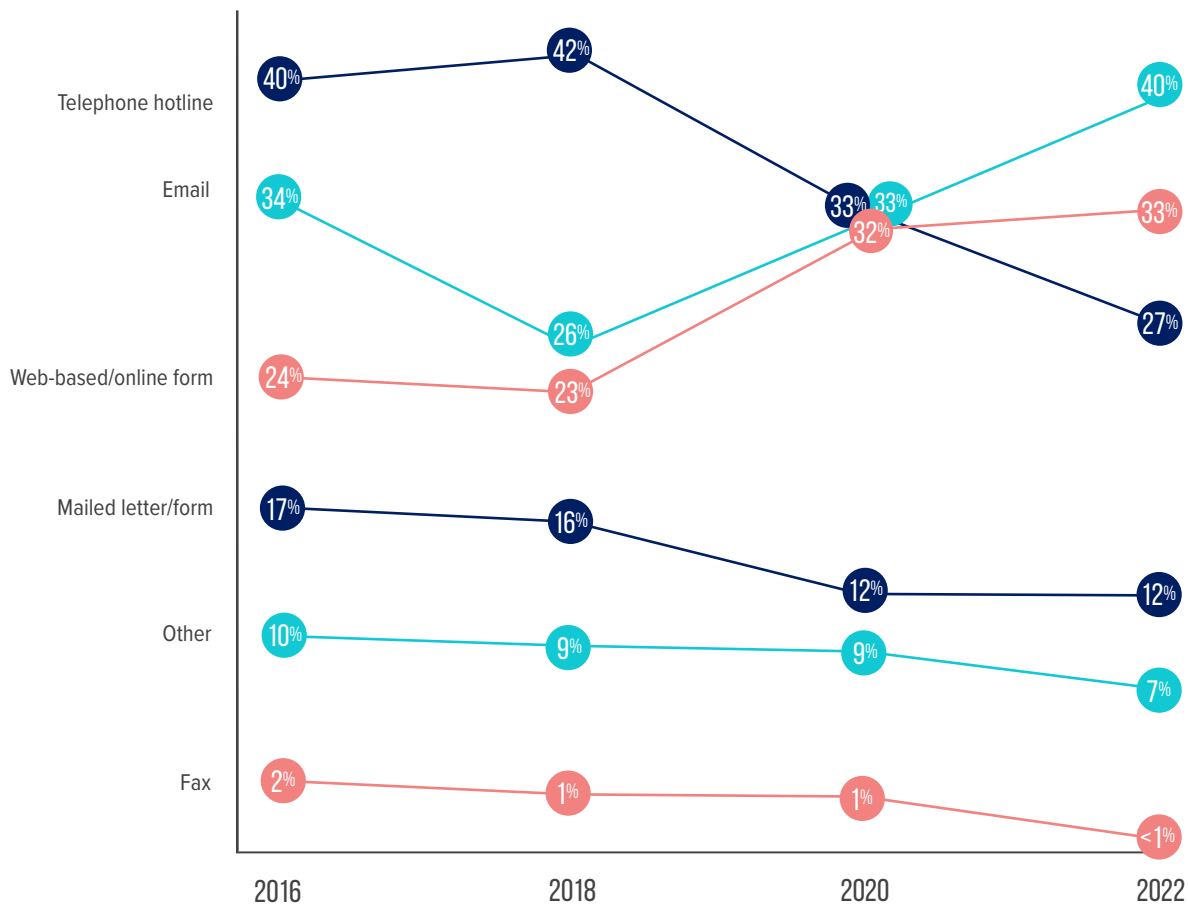
HOTLINE IMPLEMENTATION AND TIP DETECTION RATES BY REGION



REPORTING MECHANISMS

In cases where a reporting mechanism was used to report fraud, we asked respondents to specify how the tip arrived. In our previous studies, telephone hotlines were the most common mechanism whistleblowers used. However, as shown in Figure 13, telephone hotline use has declined substantially, while email and web-based/online reporting have both surpassed telephone hotlines. These findings demonstrate that whistleblowers' preferred methods of reporting fraud are diverse and evolving, particularly regarding online and electronic forms. Consequently, organizations should maintain multiple channels for reporting fraud.

FIG. 13 WHAT FORMAL REPORTING MECHANISMS DID WHISTLEBLOWERS USE?



42% of frauds were detected by tips, which is nearly **3x** as many cases as the next most common method

More than **HALF** of all tips came from employees



PARTIES TO WHOM WHISTLEBLOWERS REPORT

Not all tips about suspected fraud are reported through a formal reporting mechanism. Some reports are made informally to individuals within the organization. Figure 14 indicates that whistleblowers who do not use hotline mechanisms are most likely to report their concerns to their direct supervisors (30%). But this chart also makes clear that whistleblowers may reach out to a wide variety of parties, such as executives, internal audit, fraud investigation teams, or their coworkers. Because almost anyone in an organization could potentially receive a report, it is important to provide all staff with guidance on how fraud allegations are handled within the organization and what to do if they receive a report about suspected fraud.

FIG. 14 TO WHOM DID WHISTLEBLOWERS INITIALLY REPORT?



VICTIM ORGANIZATIONS



To determine how the impact of fraud varies among victim organizations, we asked survey participants about the victim organizations in their cases, including their size, type, industry, and which anti-fraud controls they had in place when the schemes occurred.

TYPE OF ORGANIZATION

More than two-thirds (69%) of frauds reported by our survey respondents occurred in for-profit organizations, with 44% of the victim organizations being private companies and 25% being public companies, as shown in Figure 15. Private and public companies suffered a median loss of USD 120,000 and USD 118,000, respectively. Nonprofit organizations were the victims in only 9% of the reported fraud cases and suffered the smallest median loss of USD 60,000.

Government agencies at different levels can vary widely in terms of their operations, personnel, and budgets, and therefore tend to be impacted differently by fraud. To analyze this, we separated the government organizations in our study by level. National-level entities represented the highest number of reported frauds (46%) and had the greatest median loss of USD 200,000, which is nearly four times the median loss incurred by state/provincial-level entities (USD 56,000). Additionally, local governments, which tend to be smaller in terms of staffing and resources, suffered the second-highest median loss of USD 125,000, more than twice as much as state/provincial-level entities.

FIG. 15 WHAT TYPES OF ORGANIZATIONS ARE VICTIMIZED BY OCCUPATIONAL FRAUD?

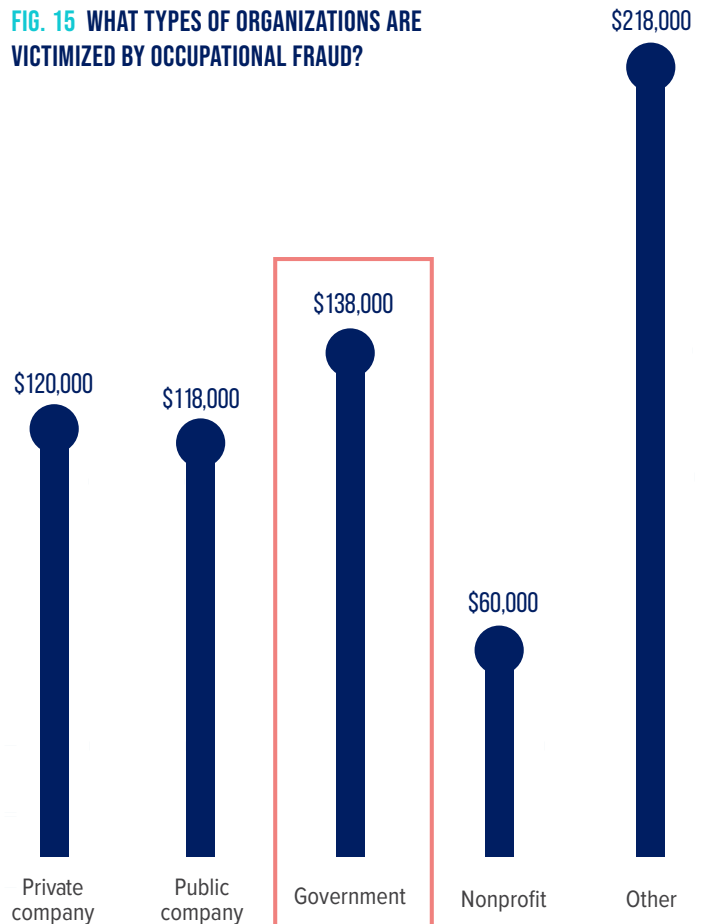
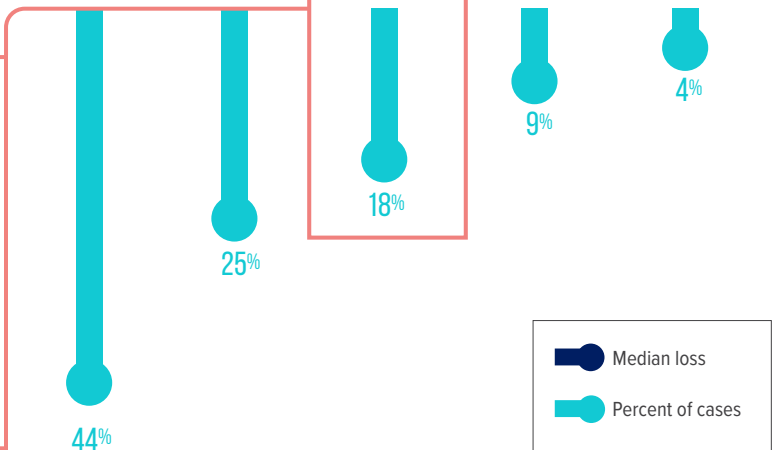
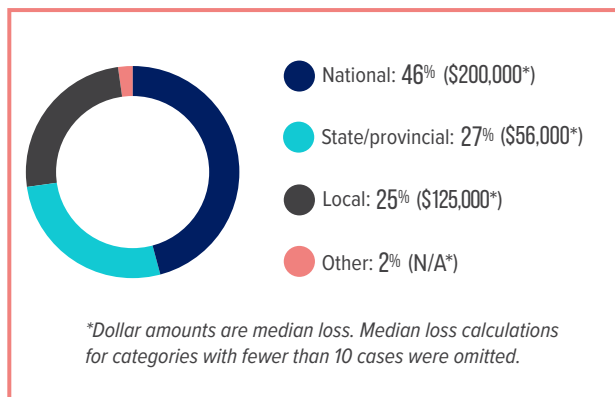


FIG. 16 WHAT LEVELS OF GOVERNMENT ARE VICTIMIZED BY OCCUPATIONAL FRAUD?



SIZE OF ORGANIZATION

In Figure 17, we categorized all victim organizations based on their number of employees. Small businesses (fewer than 100 employees) had the highest median loss of USD 150,000, while the largest organizations (more than 10,000 employees) had a median loss of USD 138,000. Even though the median loss figures for small and large organizations were similar, the impact of such a loss is likely far more significant at a smaller organization.

FIG. 17 HOW DOES AN ORGANIZATION'S SIZE RELATE TO ITS OCCUPATIONAL FRAUD RISK?

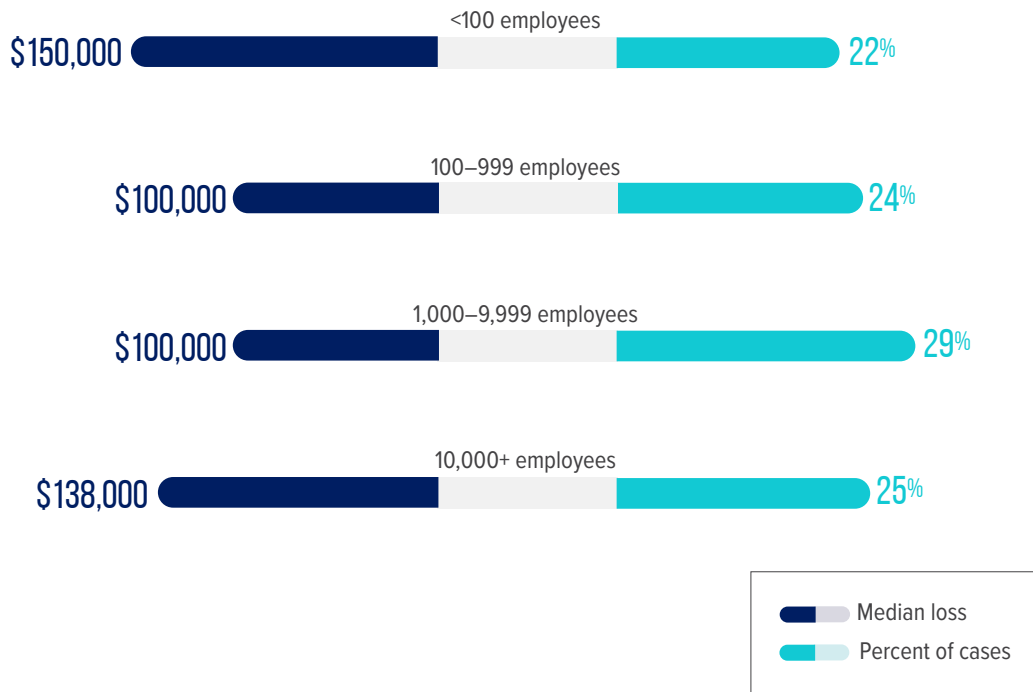
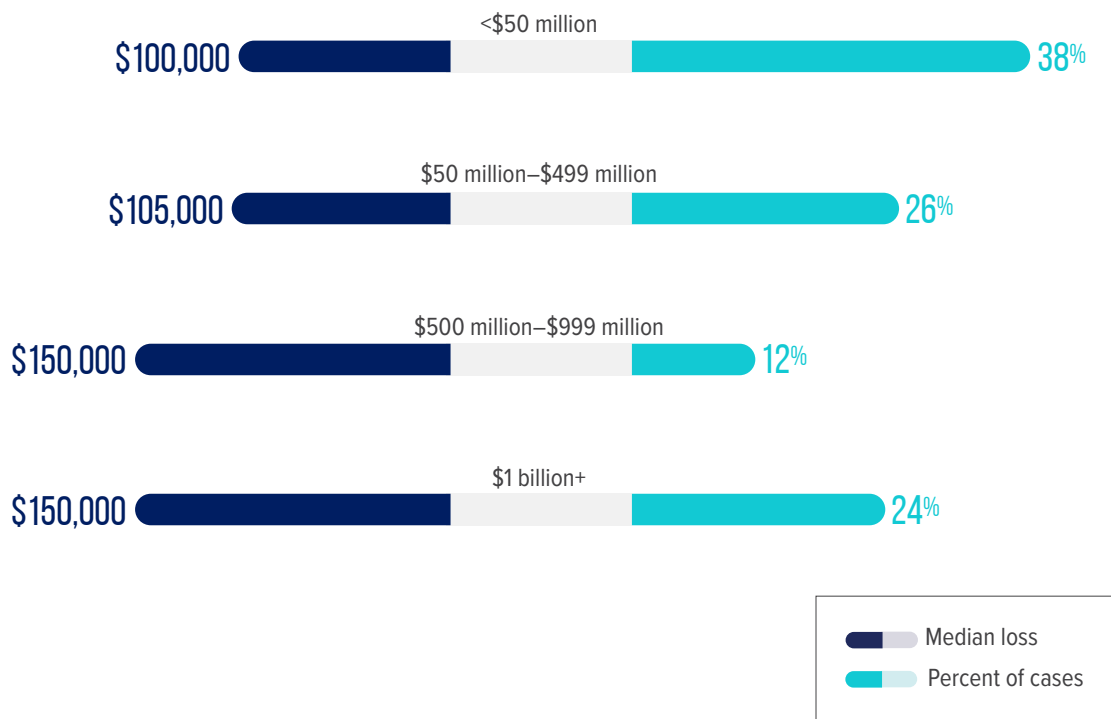
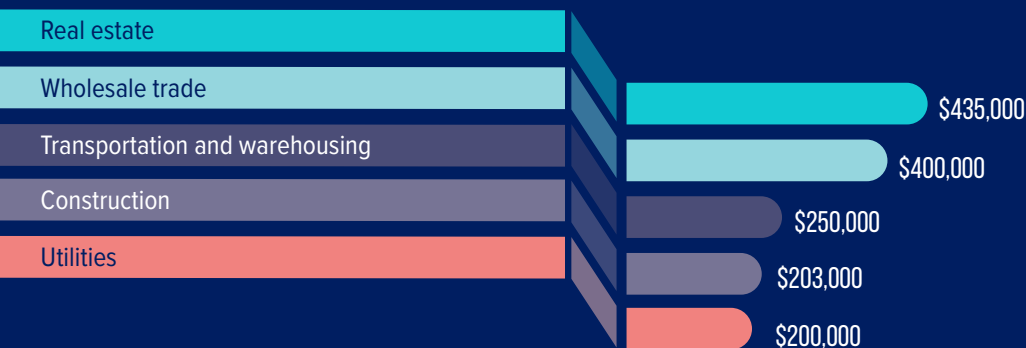


Figure 18 shows the distribution of victim organizations based on revenue size. Median losses ranged from USD 100,000 in the smallest organizations to USD 150,000 in the largest. But again, an organization with less than USD 50 million in annual revenue is likely to feel that impact much more than an organization with a revenue of USD 1 billion or more.

FIG. 18 HOW DOES AN ORGANIZATION'S GROSS ANNUAL REVENUE RELATE TO ITS OCCUPATIONAL FRAUD RISK?



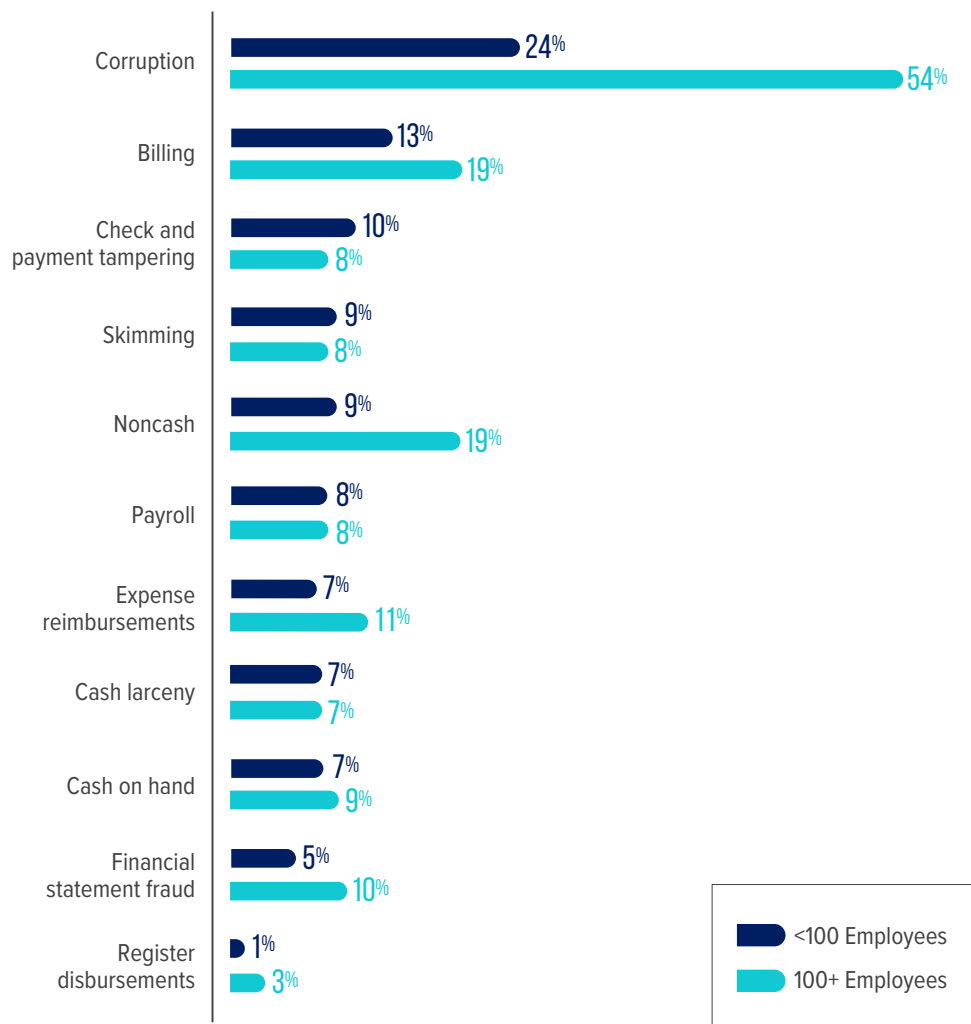
TOP 5 MEDIAN LOSSES BY INDUSTRY



ORGANIZATIONS WITH THE FEWEST EMPLOYEES HAD THE HIGHEST MEDIAN LOSS (\$150,000)

In Figure 19, we compare the frequency of schemes in small businesses (i.e., those with fewer than 100 employees) and larger organizations (i.e., those with more than 100 employees). The most significant difference involves corruption, which is much more prevalent in larger organizations than smaller ones (54% and 24%, respectively). Misappropriation of noncash assets was also more than twice as common in larger organizations. Only two schemes occurred more frequently in smaller organizations than larger organizations: skimming and check and payment tampering.

FIG. 19 HOW DO FRAUD SCHEMES VARY BY ORGANIZATION SIZE?



INDUSTRY OF ORGANIZATION

Survey participants were asked to identify the victim organization's industry. The industries affected by the greatest number of cases in our study were banking and financial services, government and public administration, and manufacturing. It is important to note that this does not necessarily mean that more fraud occurs in these industries; rather, it might indicate that these industries employ more CFEs than others. The real estate industry suffered the highest median loss of USD 435,000, followed by the wholesale trade sector with the next-highest median loss of USD 400,000.

FIG. 20 HOW DOES OCCUPATIONAL FRAUD AFFECT ORGANIZATIONS IN DIFFERENT INDUSTRIES?



MOST COMMON SCHEMES BY INDUSTRY

Identifying the frequency of various fraud schemes within industries could help organizations in those industries determine which controls to implement. The heat map in Figure 21 shows the most common types of schemes that occurred in industries with more than 50 reported cases. The risks are shaded from light to dark blue, with darker variants representing higher-risk areas. For example, the most common fraud scheme in the retail industry was corruption (43%), followed by noncash schemes (24%); its lowest area of risk was financial statement fraud (4%).

FIG. 21 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	351	10%	11%	14%	14%	46%	8%	11%	11%	4%	2%	10%
Government and public administration	198	21%	8%	7%	9%	57%	12%	8%	16%	16%	3%	8%
Manufacturing	194	26%	5%	9%	7%	59%	10%	12%	23%	10%	4%	8%
Health care	130	20%	6%	8%	8%	50%	11%	9%	18%	12%	2%	9%
Energy	97	24%	9%	6%	8%	64%	16%	8%	13%	6%	3%	2%
Retail	91	19%	10%	9%	9%	43%	7%	4%	24%	5%	7%	14%
Insurance	88	15%	9%	8%	10%	40%	9%	5%	8%	10%	2%	11%
Technology	84	21%	6%	10%	6%	54%	14%	8%	30%	5%	1%	1%
Transportation and warehousing	82	20%	9%	15%	4%	59%	11%	7%	22%	9%	4%	11%
Construction	78	24%	8%	10%	14%	56%	17%	18%	24%	24%	3%	9%
Education	69	26%	9%	12%	12%	49%	12%	12%	19%	14%	4%	12%
Information	60	15%	5%	5%	8%	58%	12%	12%	33%	7%	2%	7%
Food service and hospitality	52	19%	10%	21%	17%	54%	13%	13%	29%	19%	10%	17%

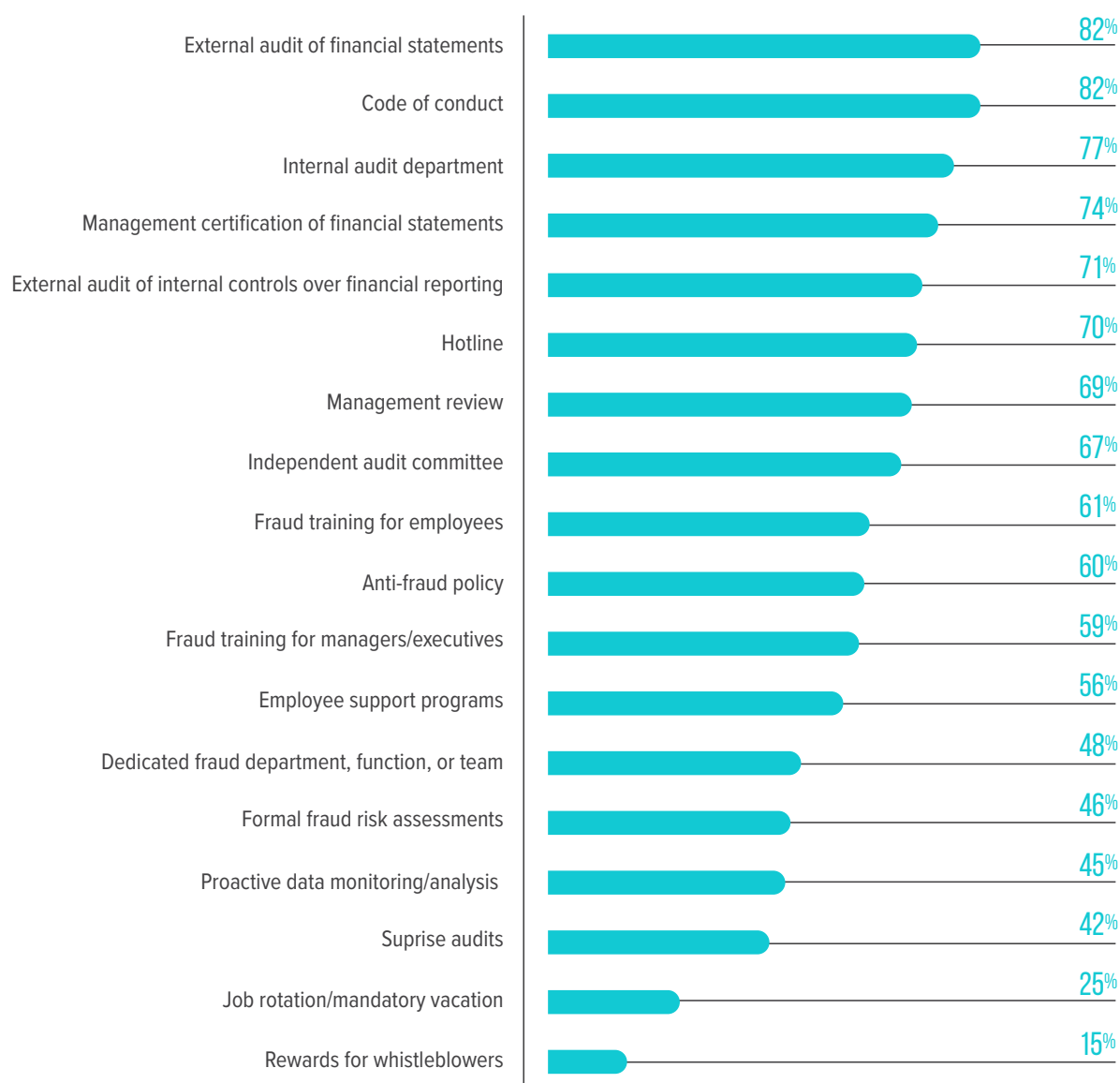


ANTI-FRAUD CONTROLS AT VICTIM ORGANIZATIONS

Fraud doesn't happen in a vacuum; organizations often enact specific internal controls designed to prevent, detect, or mitigate any attempted wrongdoing. However, the effectiveness of these measures in deterring and uncovering fraud can depend on many factors and can change over time. Consequently, it can be helpful for organizations to benchmark their own anti-fraud controls against those of other organizations.

We asked survey respondents which, if any, of 18 common anti-fraud controls the victim organization had in place at the time the fraud occurred. As shown in Figure 22, the two most common of these controls were external (independent) audits of financial statements and a formal code of conduct, each of which were implemented in 82% of the victim organizations. Other common controls include an internal audit department (77%), management certification of financial statements (74%), and an external (independent) audit of the internal controls over financial reporting (71%).

FIG. 22 WHAT ANTI-FRAUD CONTROLS ARE MOST COMMON?



EFFECTIVENESS OF ANTI-FRAUD CONTROLS

To help evaluate the effectiveness of these 18 anti-fraud controls, we compared the median losses and median durations in cases in which the victim organization had the control in place against cases in which the victim organization lacked the control. The results of these analyses are reflected in Figures 23 and 24. As noted, the presence of all 18 controls was associated with a lower median loss, and all but one control (employee support programs) was correlated with faster fraud detection.

In particular, two controls—job rotation/mandatory vacation policies and surprise audits—were associated with at least a 50% reduction in both median loss and median duration. Interestingly, these are among the least common controls implemented, with only 25% of organizations having a job rotation/mandatory vacation policy and 42% using surprise audits, indicating that numerous organizations have an opportunity to add these highly effective tools to their anti-fraud programs. Other controls with notable reductions in both measures include proactive data monitoring/analysis and formal fraud risk assessments.

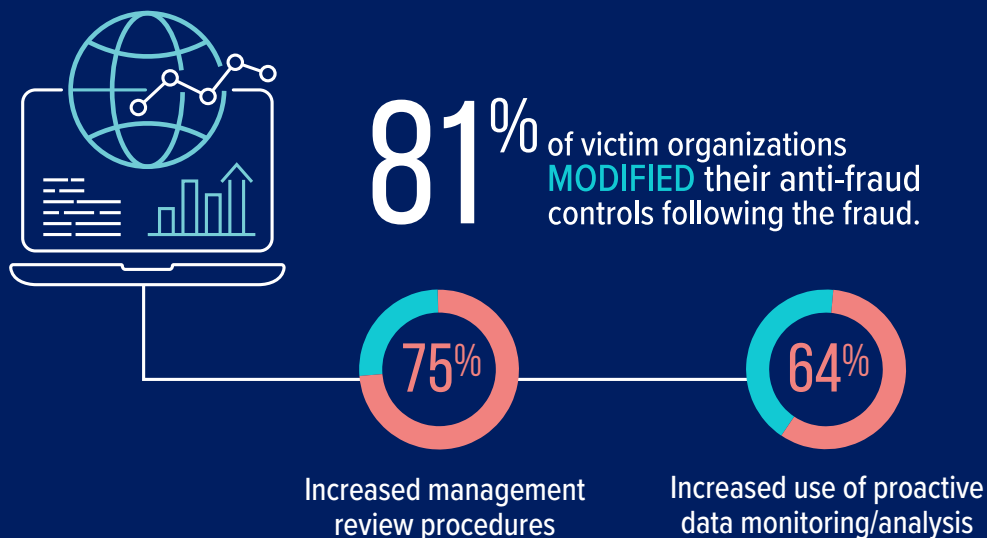
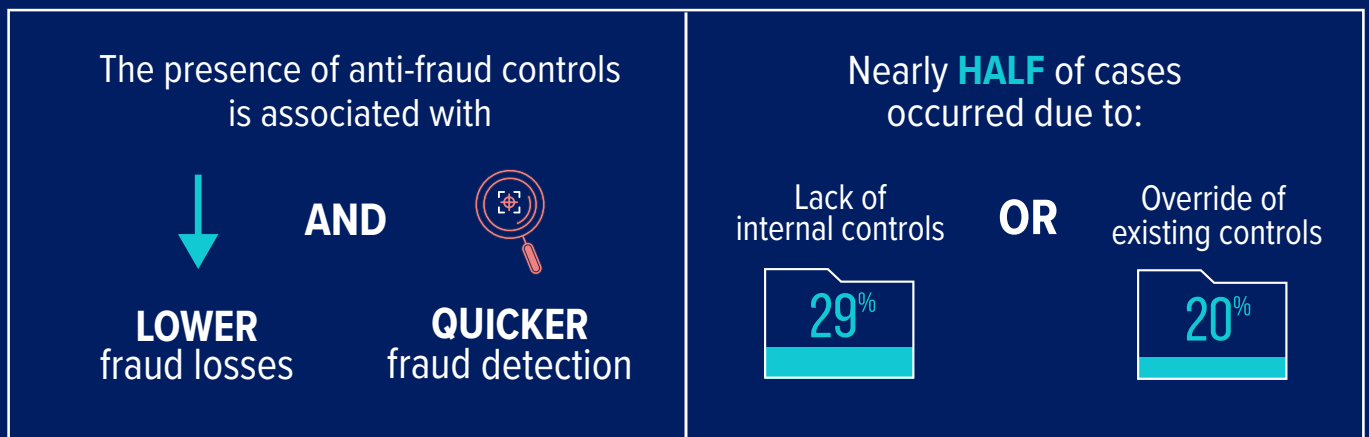
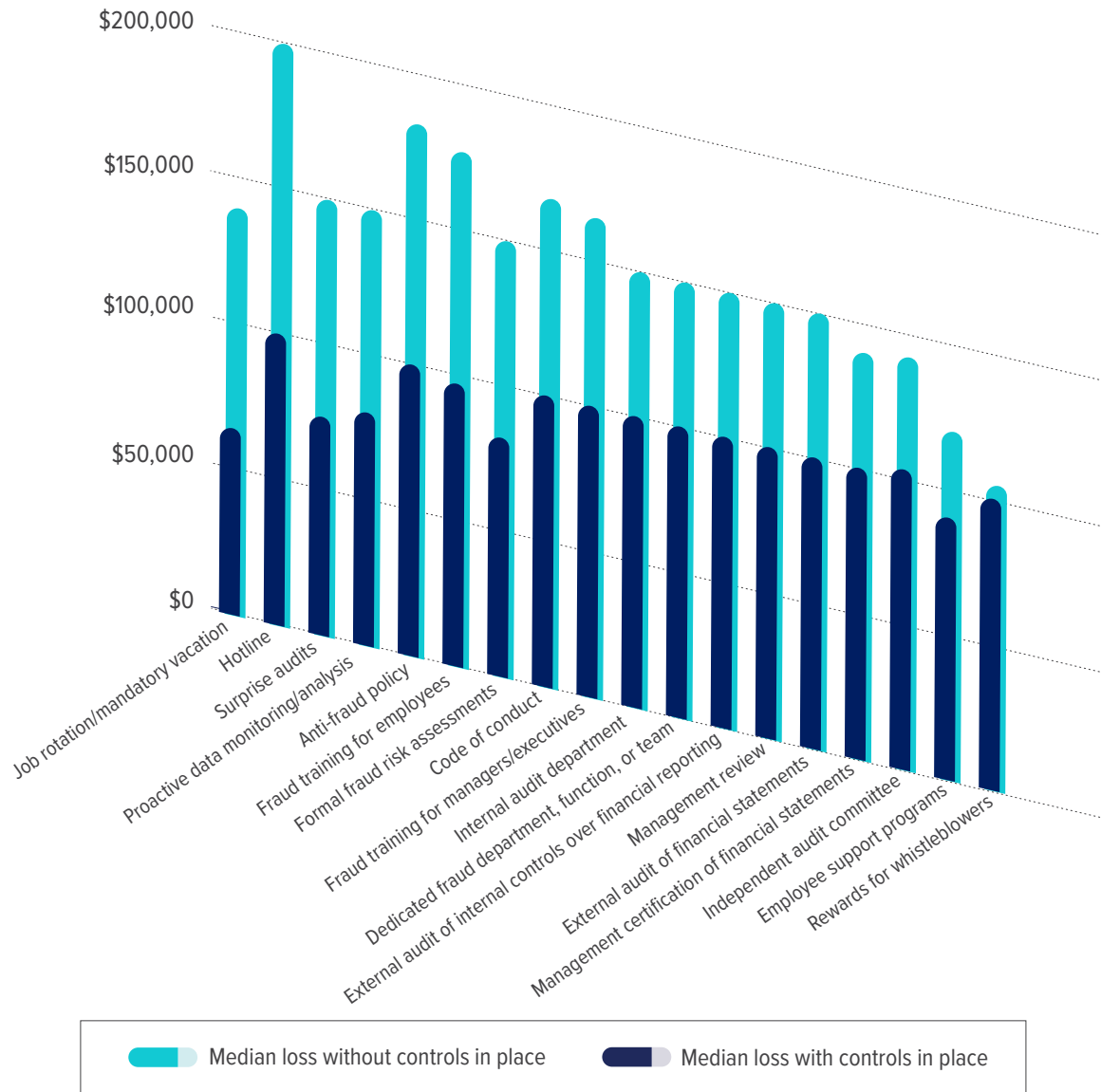
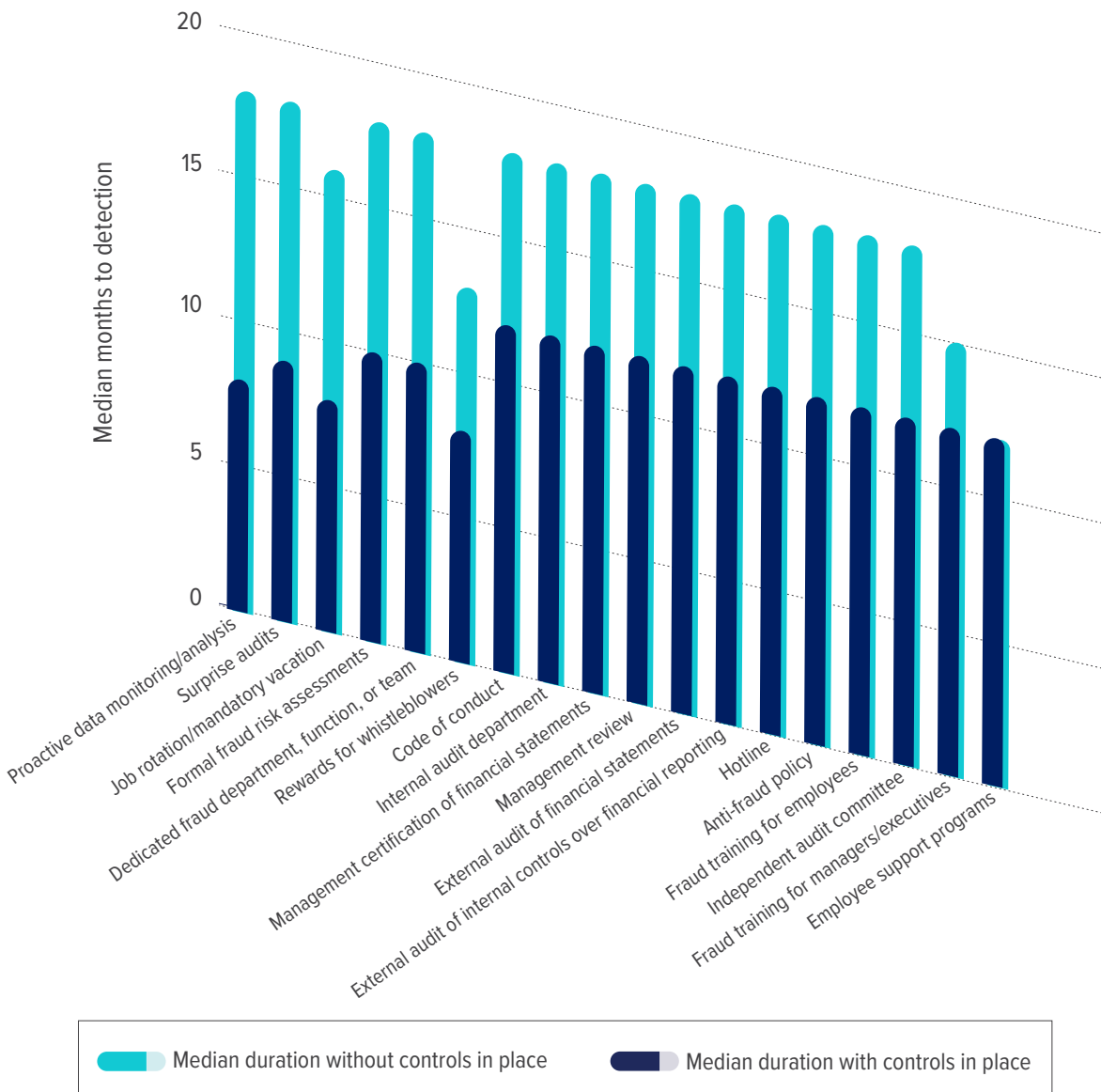


FIG. 23 HOW DOES THE PRESENCE OF ANTI-FRAUD CONTROLS RELATE TO MEDIAN LOSS?



Control	Percent of cases	Control in place	Control not in place	Percent reduction
Job rotation/mandatory vacation	25%	\$ 64,000	\$140,000	54%
Hotline	70%	\$100,000	\$200,000	50%
Surprise audits	42%	\$ 75,000	\$150,000	50%
Proactive data monitoring/analysis	45%	\$ 80,000	\$150,000	47%
Anti-fraud policy	60%	\$100,000	\$183,000	45%
Fraud training for employees	61%	\$ 97,000	\$177,000	45%
Formal fraud risk assessments	46%	\$ 82,000	\$150,000	45%
Code of conduct	82%	\$100,000	\$168,000	40%
Fraud training for managers/executives	59%	\$100,000	\$165,000	39%
Internal audit department	77%	\$100,000	\$150,000	33%
Dedicated fraud department, function, or team	48%	\$100,000	\$150,000	33%
External audit of internal controls over financial reporting	71%	\$100,000	\$150,000	33%
Management review	69%	\$100,000	\$150,000	33%
External audit of financial statements	82%	\$100,000	\$150,000	33%
Management certification of financial statements	74%	\$100,000	\$140,000	29%
Independent audit committee	67%	\$103,000	\$142,000	27%
Employee support programs	56%	\$ 90,000	\$120,000	25%
Rewards for whistleblowers	15%	\$100,000	\$105,000	5%

FIG. 24 HOW DOES THE PRESENCE OF ANTI-FRAUD CONTROLS RELATE TO THE DURATION OF FRAUD?



Control	Percent of cases	Control in place	Control not in place	Percent reduction
Proactive data monitoring/analysis	45%	8 months	18 months	56%
Surprise audits	42%	9 months	18 months	50%
Job rotation/mandatory vacation	25%	8 months	16 months	50%
Formal fraud risk assessments	46%	10 months	18 months	44%
Dedicated fraud department, function, or team	48%	10 months	18 months	44%
Rewards for whistleblowers	15%	8 months	13 months	38%
Code of conduct	82%	12 months	18 months	33%
Internal audit department	77%	12 months	18 months	33%
Management certification of financial statements	74%	12 months	18 months	33%
Management review	69%	12 months	18 months	33%
External audit of financial statements	82%	12 months	18 months	33%
External audit of internal controls over financial reporting	71%	12 months	18 months	33%
Hotline	70%	12 months	18 months	33%
Anti-fraud policy	60%	12 months	18 months	33%
Fraud training for employees	61%	12 months	18 months	33%
Independent audit committee	67%	12 months	18 months	33%
Fraud training for managers/executives	59%	12 months	15 months	20%
Employee support programs	56%	12 months	12 months	0%

ANTI-FRAUD CONTROLS IN SMALL BUSINESSES

Small organizations face unique challenges in combatting fraud—from limited financial resources and smaller staff sizes that require many individuals to perform numerous functions, to the large amount of trust needed to keep operations running and the business growing. Unfortunately, that means that many of the protective anti-fraud controls that larger organizations rely on are simply not enacted within small businesses. Figure 25 shows the implementation rates of anti-fraud controls at small businesses (i.e., organizations with fewer than 100 employees) compared to their larger counterparts. Across all 18 controls, small organizations had notably lower levels of implementation; even the most common controls—external audits of financial statements and a formal code of conduct—were only in place at 53% of small businesses in our study, compared to approximately 90% of larger organizations.

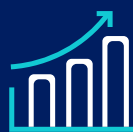
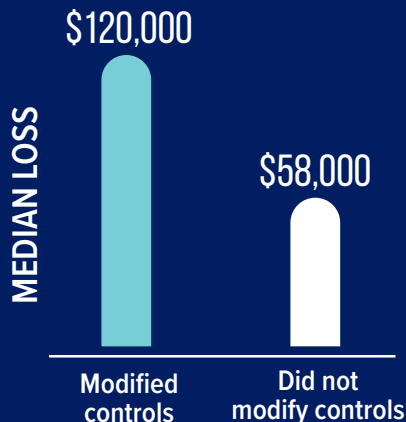
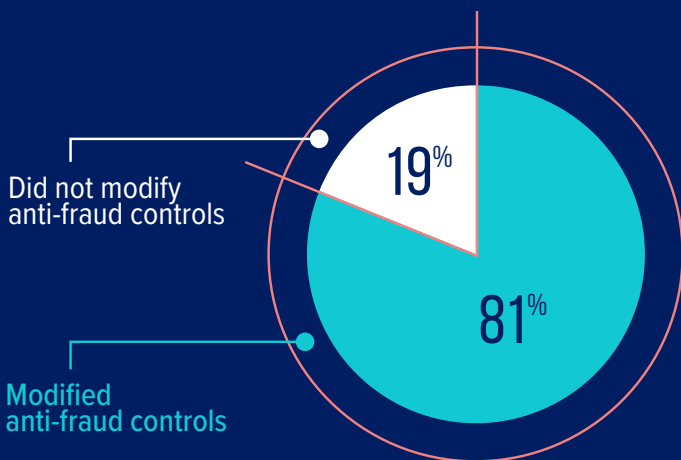
FIG. 25 HOW DO ANTI-FRAUD CONTROLS VARY BY SIZE OF VICTIM ORGANIZATION?



MODIFYING ANTI-FRAUD CONTROLS FOLLOWING A FRAUD

A comprehensive response to a discovered fraud should include assessing the factors that allowed the fraud to occur and taking steps to prevent similar frauds from being able to happen again in the future.

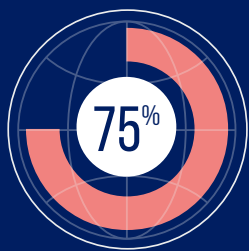
DID VICTIM ORGANIZATIONS MODIFY THEIR ANTI-FRAUD CONTROLS FOLLOWING FRAUD?



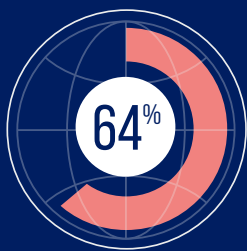
ORGANIZATIONS THAT HAD HIGHER LOSSES were more likely to modify their controls following the fraud

MOST COMMON CHANGES MADE TO ANTI-FRAUD CONTROLS

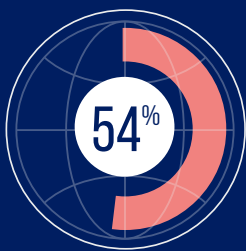
Of changes made to anti-fraud controls, the most common involved implementing or modifying:



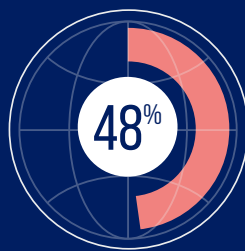
Management review



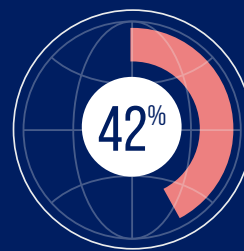
Proactive data monitoring



Surprise audits



Internal audit department



Anti-fraud training



WHICH TYPES OF ORGANIZATIONS WERE MOST LIKELY TO MODIFY THEIR ANTI-FRAUD CONTROLS?

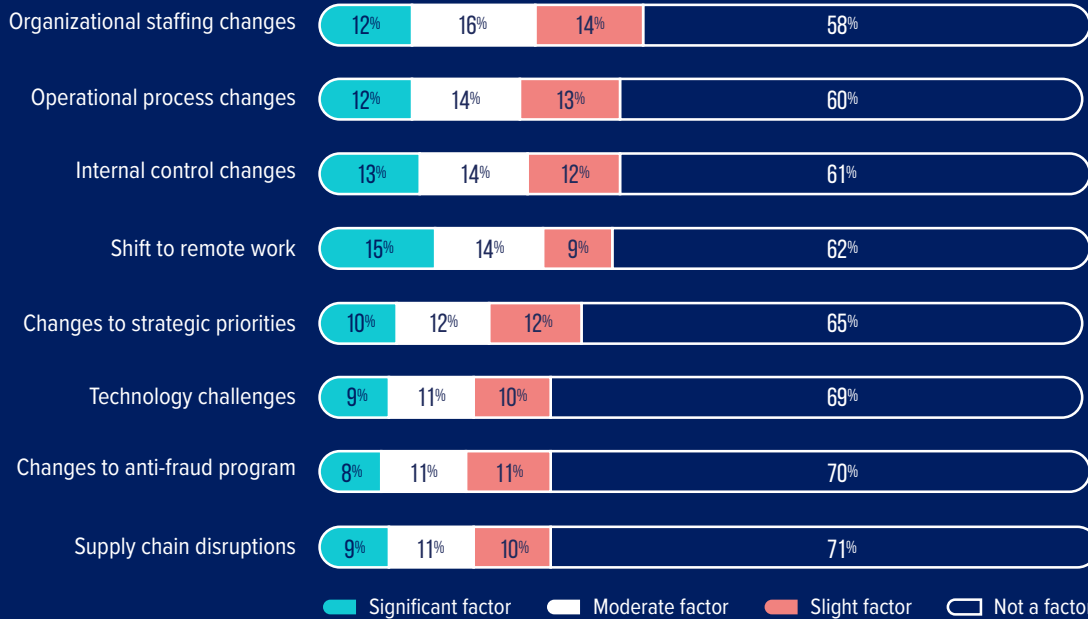


COVID'S EFFECT ON OCCUPATIONAL FRAUD

We asked survey participants whether several pandemic-related issues contributed to the frauds that they investigated; 52% of respondents noted that at least one of these factors was present in their case. Of the factors analyzed, pandemic-related organizational staffing changes were the most common (42% of cases), and a shift to remote work was the factor most commonly cited as significant (15% of cases).



TO WHAT EXTENT DID PANDEMIC-RELATED FACTORS CONTRIBUTE TO OCCUPATIONAL FRAUDS?



It's important to note that this study analyzes cases that were *investigated* between January 2020 and September 2021, not necessarily frauds that were committed during that time. Since the median duration of the frauds in this study was 12 months, many of the frauds analyzed were perpetrated before the COVID-19 pandemic began. Consequently, we anticipate seeing additional pandemic-related factors underlying the cases in our 2024 study, when many more frauds that began during the pandemic will have been detected and investigated.

BACKGROUND CHECKS

Background checks are an important tool in the fight against fraud, as they can prevent organizations from hiring individuals with known histories of misconduct. However, as noted in Figure 26, 43% of victim organizations did not run a background check on the perpetrator prior to hiring. Further, of the background checks that were run on the perpetrators, 21% revealed previous red flags, meaning that the individuals were hired even with known instances of misconduct or other concerns.

We also asked about the specific types of background checks that the victim organizations conducted. As shown in Figure 28, the two most common forms of background checks run by the organizations were employment history checks (45%) and criminal background checks (40%).

FIG. 26 WAS A BACKGROUND CHECK RUN ON THE PERPETRATOR PRIOR TO HIRING?

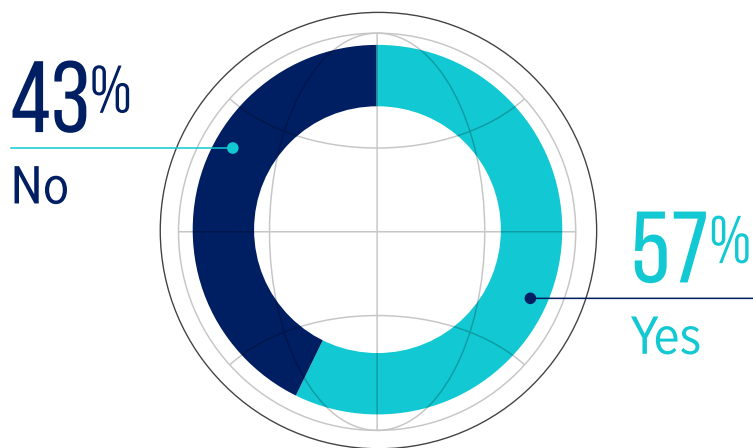


FIG. 27 DID THE BACKGROUND CHECKS REVEAL EXISTING RED FLAGS?

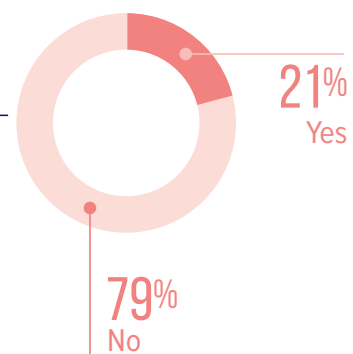


FIG. 28 WHAT TYPES OF BACKGROUND CHECKS WERE RUN ON THE PERPETRATOR PRIOR TO HIRING?



INTERNAL CONTROL WEAKNESSES THAT CONTRIBUTED TO THE FRAUD

Even in organizations with anti-fraud programs, fraud can and does happen. To better understand the factors that can lead to occupational fraud, we asked survey participants to identify the primary internal control weakness that allowed the fraud case to occur. The most common factor underlying the occupational frauds in our study was a lack of internal controls; 29% of victim organizations did not have adequate controls in place to prevent the fraud from occurring. Another 20% of cases involved an override of existing internal controls, meaning the victim organization had implemented mechanisms to protect against fraud, but the perpetrator was able to circumvent those controls. Together, this data shows that nearly half of the frauds in our study likely could have been prevented with a stronger system of anti-fraud controls.

Individuals with different levels of authority within an organization tend to have different amounts of access and influence, which can affect how they are able to perpetrate fraud. We analyzed how the internal control weaknesses varied by the position of the perpetrator, as shown in Figure 30. Not surprisingly, a poor tone at the top was the most common factor underlying schemes perpetrated by owners and executives. The most common control weakness for both staff-level employees and mid-level managers was a lack of internal controls (34% and 29%, respectively).

FIG. 29 WHAT ARE THE PRIMARY INTERNAL CONTROL WEAKNESSES THAT CONTRIBUTE TO OCCUPATIONAL FRAUD?

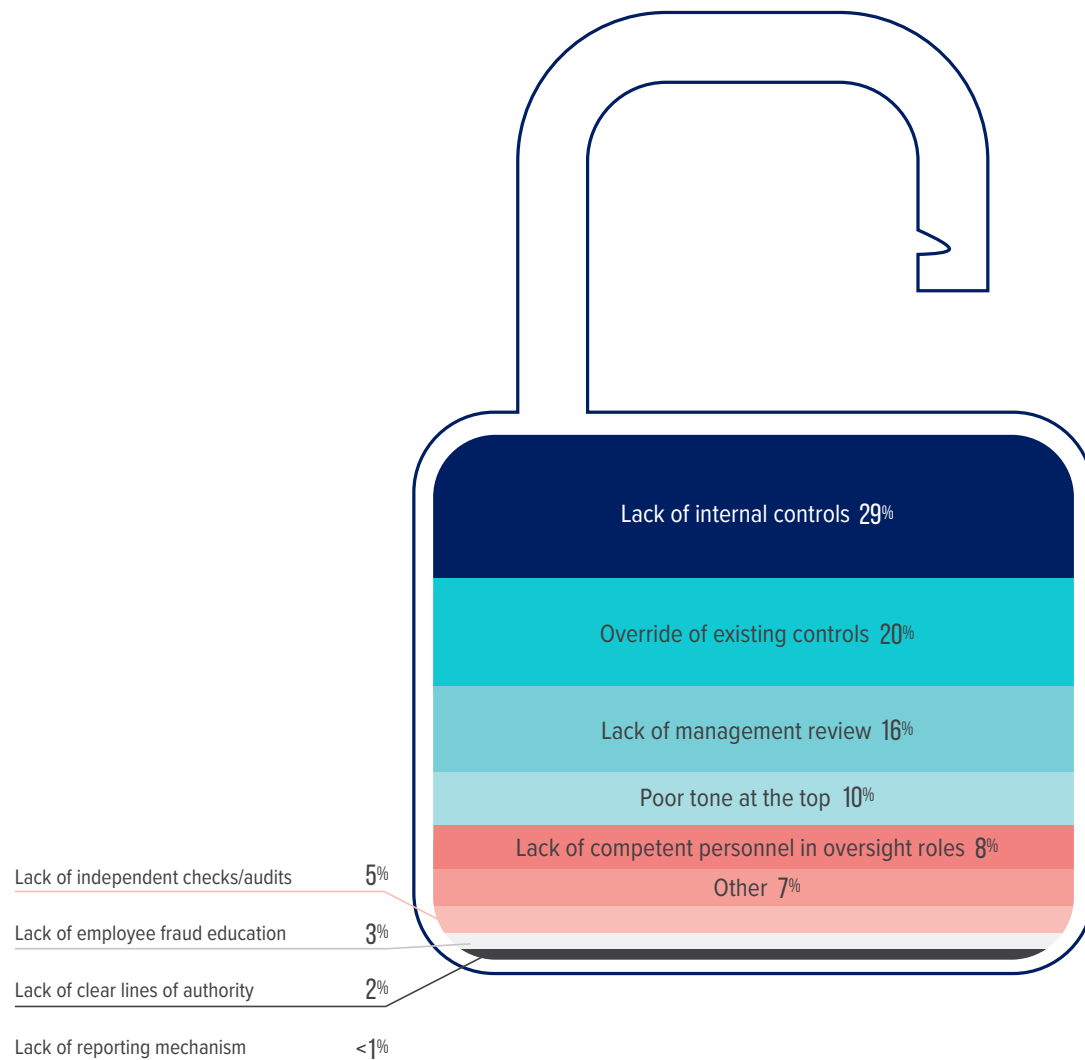
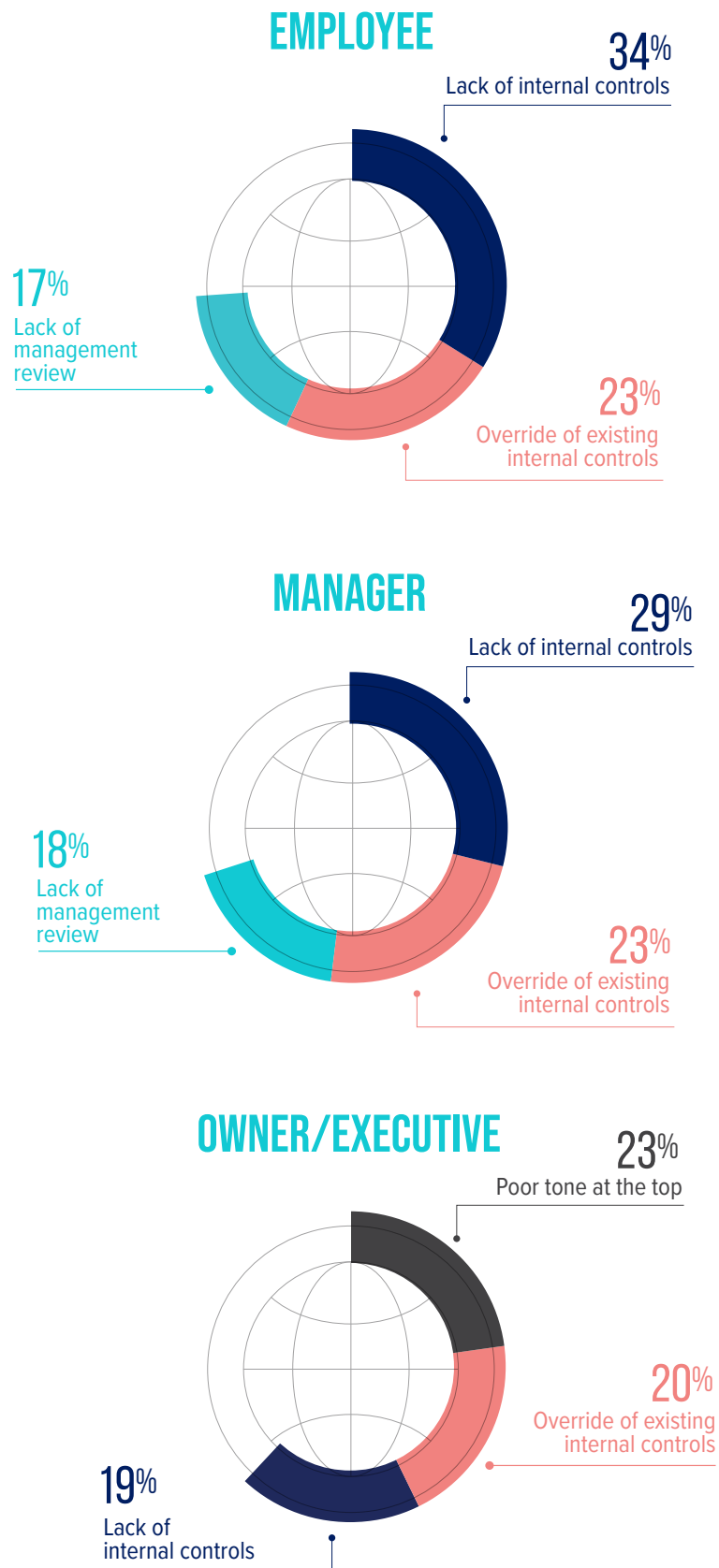


FIG. 30 TOP 3 INTERNAL CONTROL WEAKNESSES BASED ON THE PERPETRATOR'S POSITION



PERPETRATORS



Participants in our survey answered several questions about the fraud perpetrators' job details, basic demographics, prior misconduct, and behavioral warning signs that might have indicated fraud. This information helps us identify common characteristics and behaviors of fraud perpetrators, which can be used by organizations to assess relative levels of risk among their own employees.



PERPETRATOR'S POSITION

Our data shows a strong correlation between the perpetrator's level of authority and the size of the fraud. Owner/executives only committed 23% of the frauds in our study, but the median loss in those cases (USD 337,000) was significantly larger than losses caused by managers. In turn, managers caused much larger losses than staff-level employees. This finding is consistent with our past studies, all of which have shown that fraud losses tend to be larger in schemes committed by higher-level fraudsters.

Frauds committed by higher-level perpetrators also typically take longer to detect. As shown in Figure 32, the median duration of a fraud committed by an owner/executive was 18 months, whereas frauds committed by staff-level employees had a median duration of only eight months. One of the challenges of dealing with fraud committed by high-level perpetrators is that these individuals often have the ability to evade or override controls that would otherwise detect fraud. Additionally, fraudsters in positions of authority might bully or intimidate employees below them, which can deter those employees from reporting or investigating suspected wrongdoing. Both of these factors might contribute to the longer duration of frauds committed by high-level employees.

Owners/executives committed only 23% of occupational frauds, but they caused the largest losses.

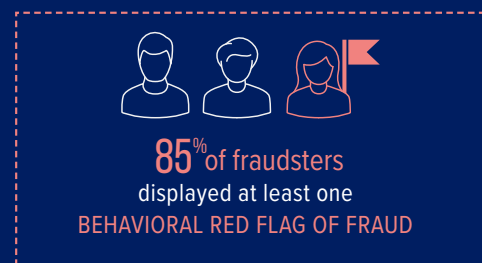
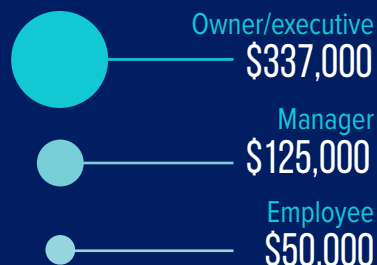


FIG. 31 HOW DOES THE PERPETRATOR'S LEVEL OF AUTHORITY RELATE TO OCCUPATIONAL FRAUD?

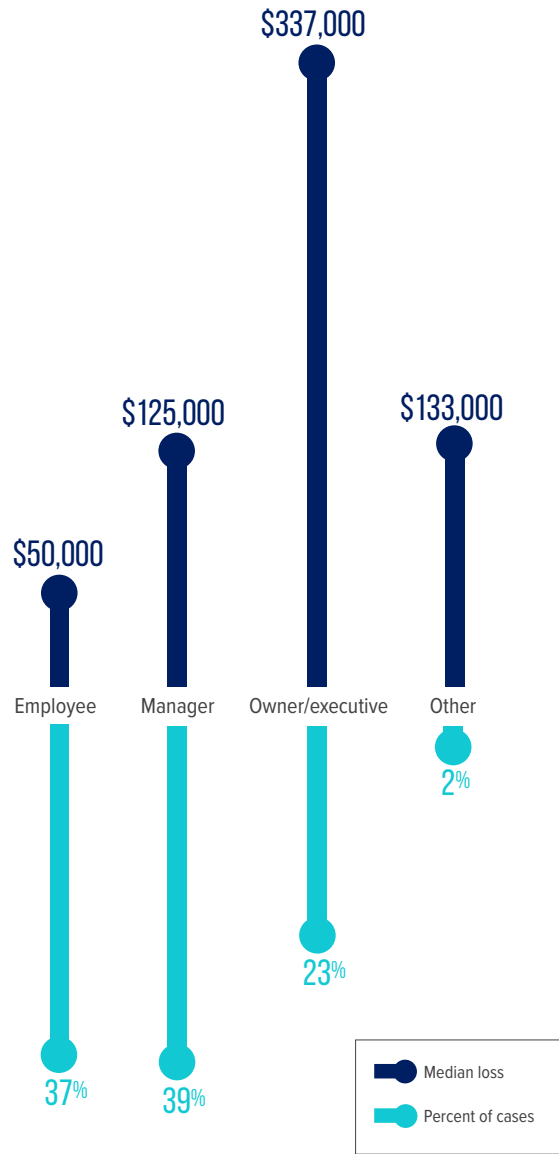
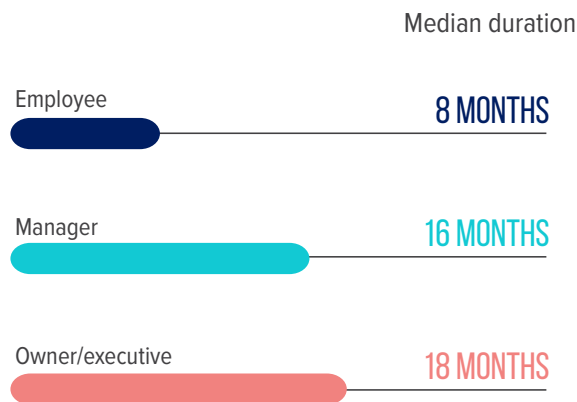


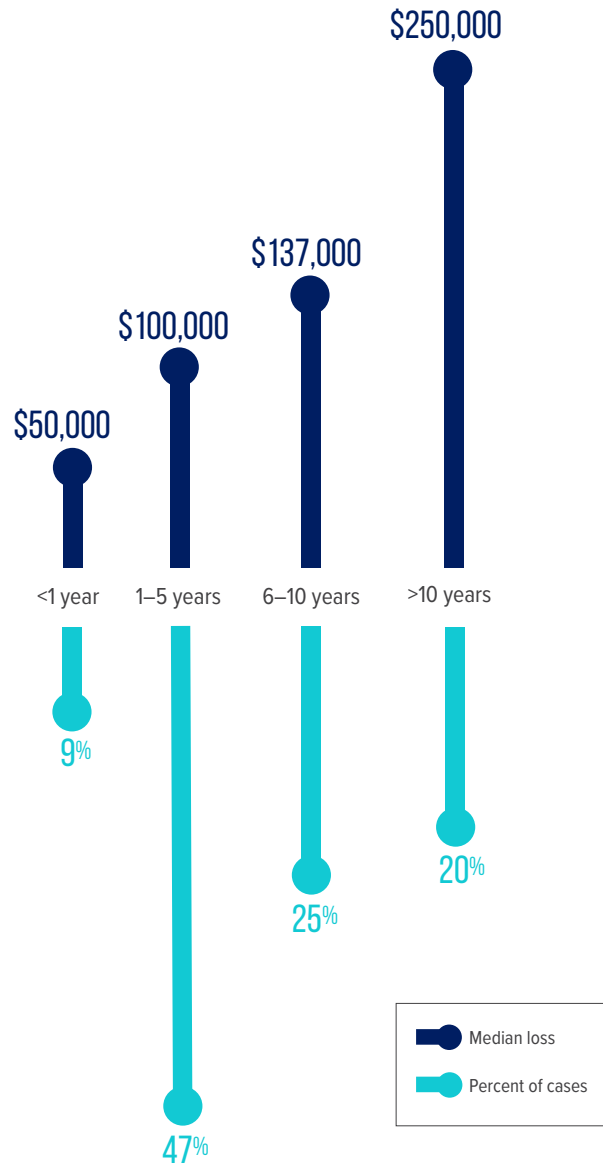
FIG. 32 HOW DOES THE PERPETRATOR'S LEVEL OF AUTHORITY RELATE TO SCHEME DURATION?



PERPETRATOR'S TENURE

The perpetrator's length of service with the victim organization is also strongly correlated with the size of the fraud. In our study, fraudsters with at least ten years of tenure at the victim organization caused median losses of USD 250,000. This was five times the median loss caused by perpetrators with less than one year of tenure.

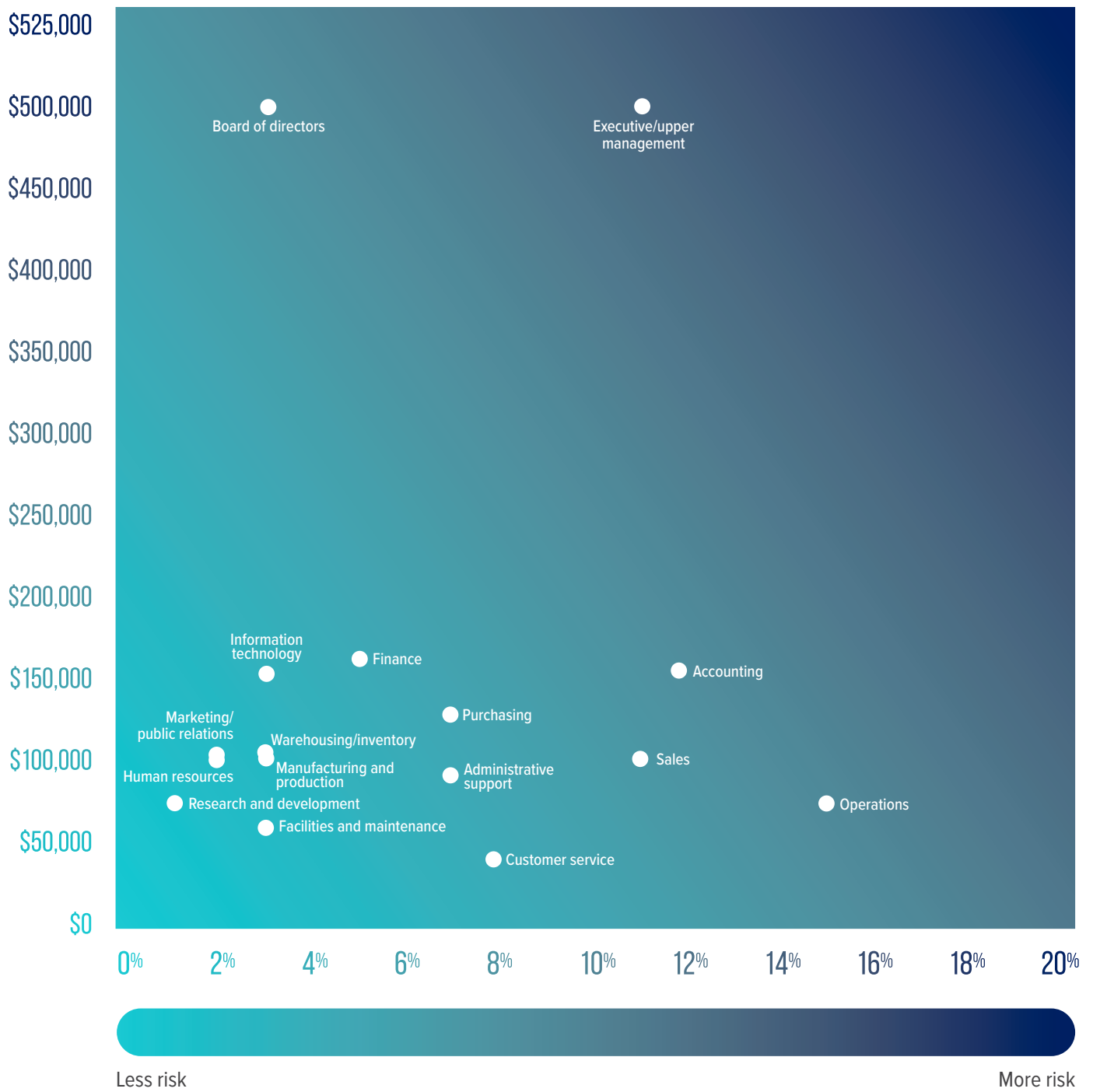
FIG. 33 HOW DOES THE PERPETRATOR'S TENURE RELATE TO OCCUPATIONAL FRAUD?



PERPETRATOR'S DEPARTMENT

In order to allocate anti-fraud controls and resources most effectively, it is important to understand the relative risks of occupational fraud throughout an organization. The heat map in Figure 34 shows the frequency and median loss of fraud schemes based on the departments in which fraud perpetrators worked. We can see, for example, that frauds committed by executives and upper management were not only common (11% of cases) but also costly (USD 500,000 median loss), making this a very high-risk area in general. Accounting and sales departments were also both associated with a high percentage of cases (12% and 11%, respectively) while also causing six-figure median losses.

FIG. 34 WHAT DEPARTMENTS POSE THE GREATEST RISK FOR OCCUPATIONAL FRAUD?



Department*	Number of cases	Percent of cases	Median loss
Operations	273	15%	\$74,000
Accounting	230	12%	\$155,000
Executive/upper management	206	11%	\$500,000
Sales	203	11%	\$100,000
Customer service	140	8%	\$40,000
Purchasing	131	7%	\$129,000
Administrative support	131	7%	\$90,000
Finance	95	5%	\$160,000

Department*	Number of cases	Percent of cases	Median loss
Board of directors	58	3%	\$500,000
Information technology	53	3%	\$150,000
Warehousing/inventory	58	3%	\$116,000
Manufacturing and production	63	3%	\$100,000
Facilities and maintenance	49	3%	\$58,000
Marketing/public relations	35	2%	\$112,000
Human resources	29	2%	\$100,000
Research and development	17	1%	\$75,000

*Departments with fewer than 10 cases were omitted.

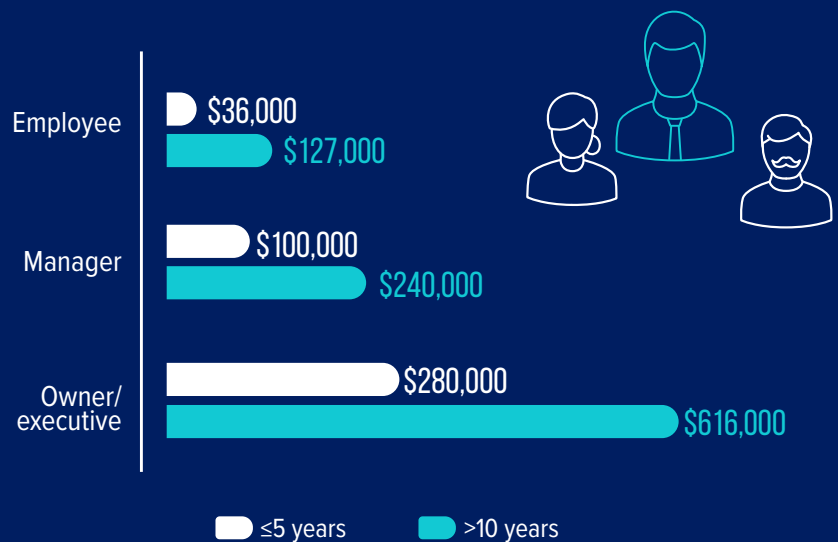
HOW DOES TENURE AFFECT FRAUD RISK?

The ability to commit fraud is a skill, and our data suggests that the longer a person works for a company, the better they become at fraud. In this infographic, we compare fraudsters with long tenure (more than 10 years) to those with moderate-to-low tenure (5 years or less).

Long-tenured **FRAUDSTERS** steal almost **3X MORE**

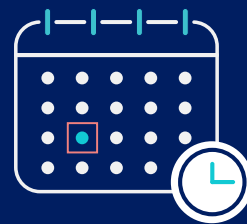
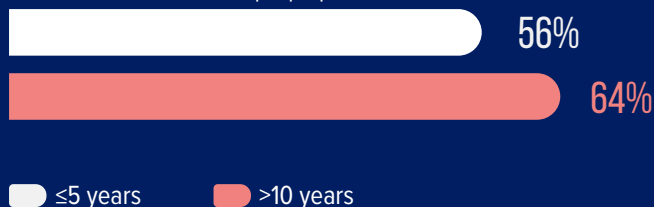


Even when **COMPARING FRAUDSTERS** with similar **LEVELS OF AUTHORITY**, **LONG-TENURED FRAUDSTERS** caused **MUCH LARGER LOSSES**



Long-tenured fraudsters are more likely to **COLLUDE**

Percent of cases with multiple perpetrators

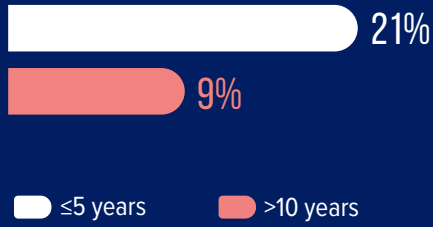


Long-tenured fraudsters **TAKE LONGER TO CATCH**

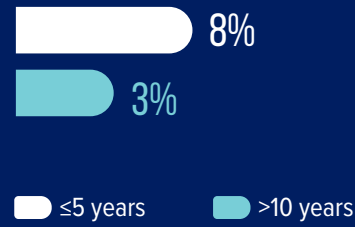




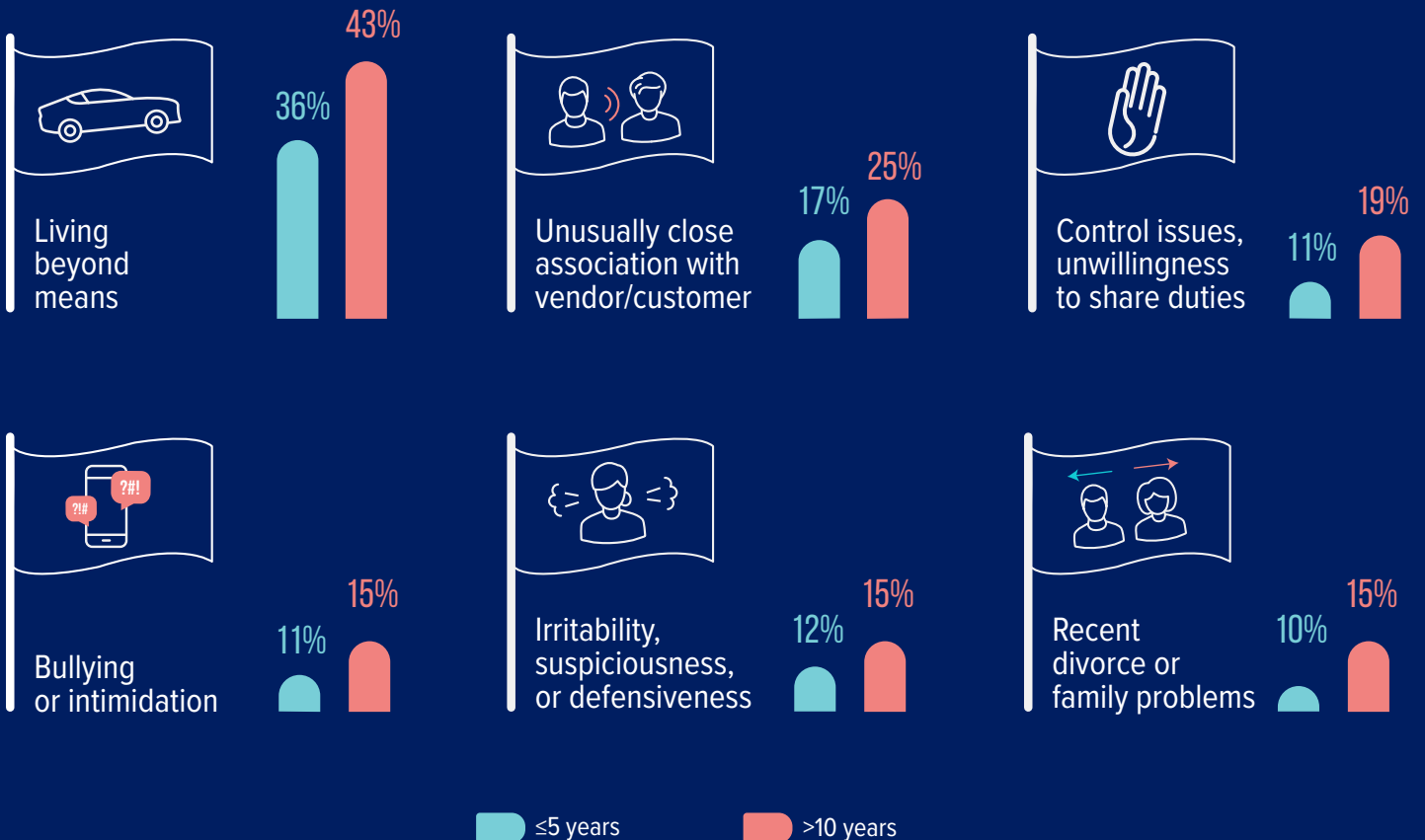
Less-tenured fraudsters were **MORE THAN TWICE AS LIKELY** to have been previously **FIRED** or **PUNISHED** for fraud-related conduct



Less-tenured fraudsters were more likely to have a **CRIMINAL RECORD**



These **6 RED FLAGS** were much more common among long-tenured employees



SCHEMES BASED ON PERPETRATOR'S DEPARTMENT

The eight departments shown in Figure 35 accounted for 76% of all occupational frauds in our study. In this chart, we have identified the frequency of various types of occupational fraud that occurred in each department. Boxes are shaded from light to dark, with darker boxes indicating higher-frequency schemes. This information can help organizations assess fraud risk and implement effective anti-fraud controls in these high-risk areas.

FIG. 35 WHAT ARE THE MOST COMMON OCCUPATIONAL FRAUD SCHEMES IN HIGH-RISK DEPARTMENTS?

DEPARTMENT	Cases	Billing	Cash larceny	Cash on hand	Check and payment tampering	Corruption	Expense reimbursements	Financial statement fraud	Noncash	Payroll	Register disbursements	Skimming
Operations	273	16%	7%	8%	11%	48%	9%	6%	16%	8%	1%	6%
Accounting	230	24%	15%	13%	29%	33%	10%	10%	7%	16%	3%	19%
Executive/upper management	206	31%	9%	10%	12%	65%	18%	22%	21%	13%	2%	12%
Sales	203	11%	6%	7%	2%	51%	8%	6%	18%	4%	2%	11%
Customer service	140	8%	10%	16%	11%	44%	6%	7%	17%	6%	3%	10%
Administrative support	131	23%	8%	15%	15%	37%	16%	5%	12%	12%	5%	10%
Purchasing	131	27%	1%	4%	2%	82%	5%	2%	14%	3%	0%	2%
Finance	95	26%	7%	11%	12%	48%	20%	14%	12%	7%	3%	12%



Nearly half of all occupational frauds came from these four departments:



Operations **15%**



Accounting **12%**



Executive/upper management **11%**

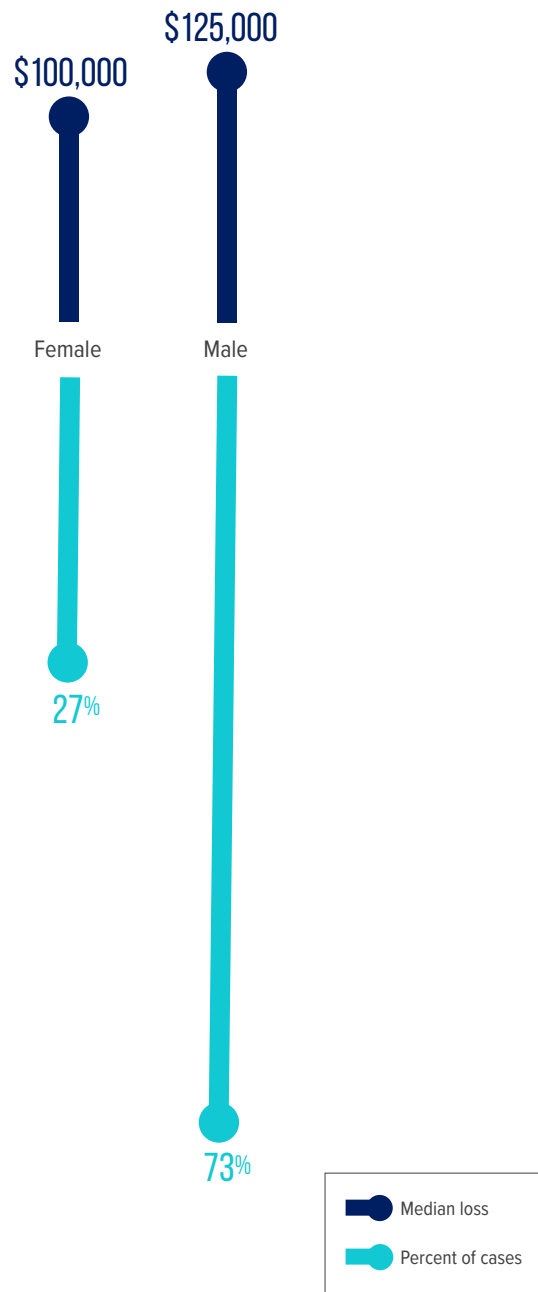


Sales **11%**

PERPETRATOR'S GENDER

As Figure 36 illustrates, 73% of occupational fraud perpetrators were male. This is consistent with our prior studies, all of which have found there to be a significant gender disparity in terms of occupational fraud frequency. However, the gap in median loss between men and women in this study was much smaller than in our previous research. Median losses caused by men (USD 125,000) were only 25% higher than median losses caused by women (USD 100,000). By comparison, in each of our prior studies, median losses caused by male perpetrators were at least 75% higher than median losses caused by female perpetrators (see A Decade of Occupational Fraud infographic, page 18).

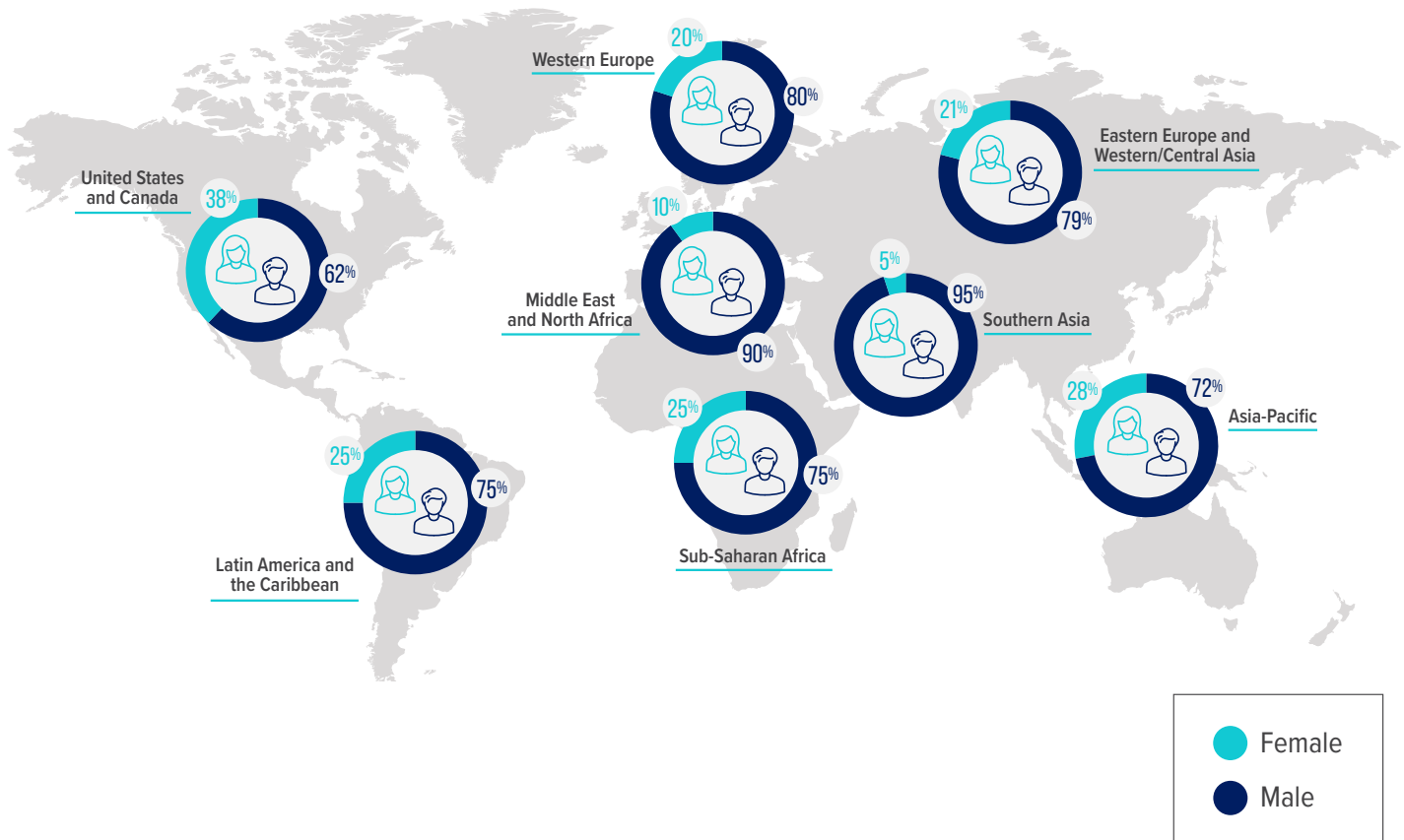
FIG. 36 HOW DOES THE PERPETRATOR'S GENDER RELATE TO OCCUPATIONAL FRAUD?



PERPETRATOR'S GENDER BASED ON REGION

The gender disparity among occupational fraudsters varied significantly based on geographic region. In the United States and Canada, for example, female perpetrators accounted for 38% of occupational frauds, while in Southern Asia and the Middle East and North Africa, female fraudsters committed a far smaller percentage of all schemes (5% and 10%, respectively).

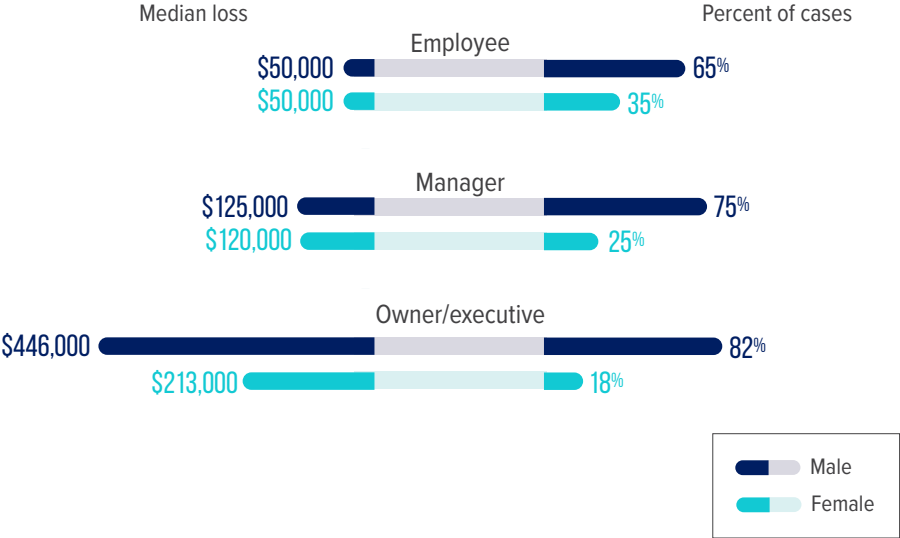
FIG. 37 HOW DOES THE GENDER DISTRIBUTION OF PERPETRATORS VARY BY REGION?



POSITION OF PERPETRATOR BASED ON GENDER

When we analyzed the cases in our study based on both the fraudster’s gender and job position, we found that men committed a much larger percentage of frauds than women did at all three levels of authority (staff-level employee, manager, and owner/executive). Interestingly, median losses for male and female perpetrators were almost identical in the employee and manager categories. It was only in the owner/executive category that fraud losses caused by men significantly exceeded those caused by women.

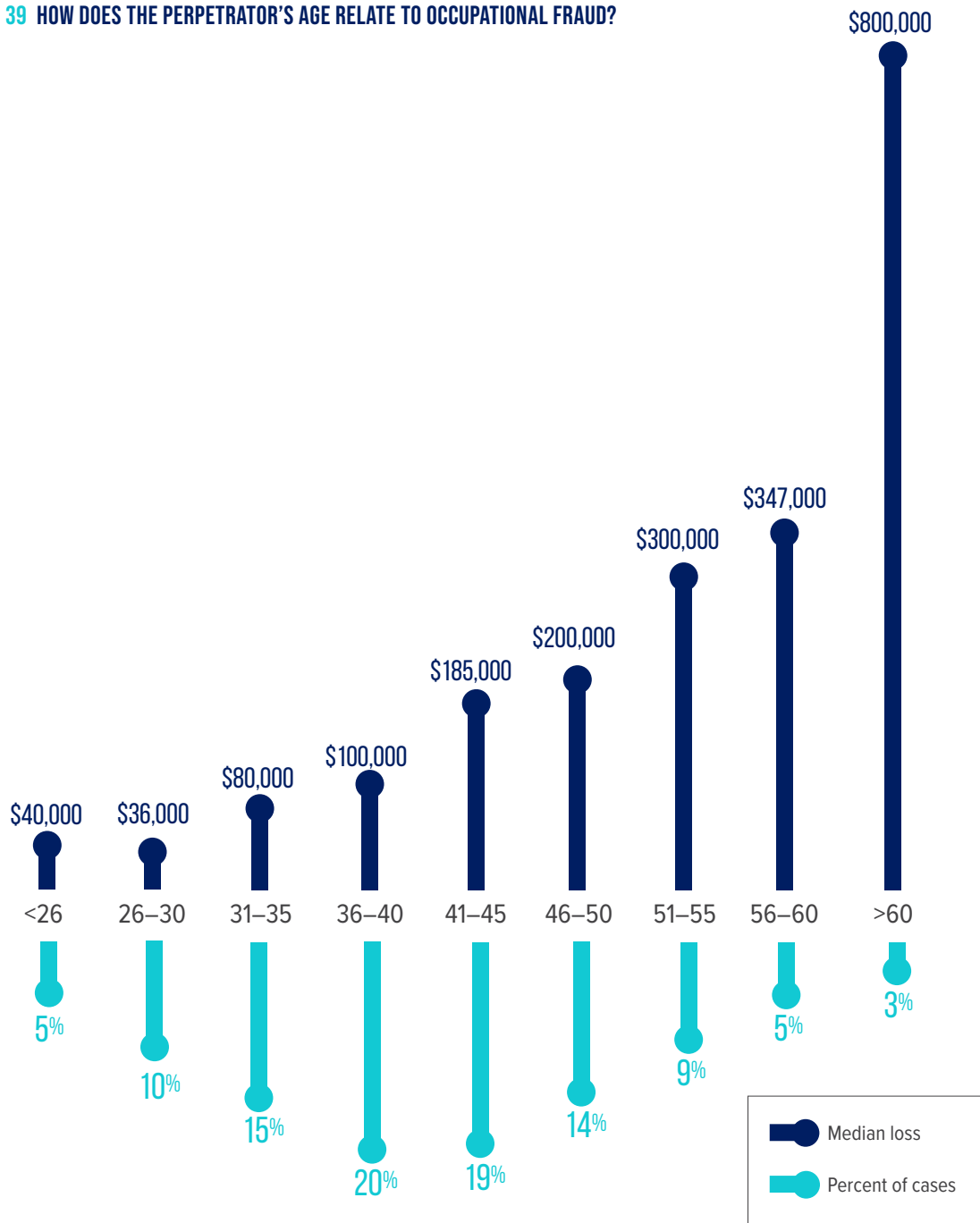
FIG. 38 HOW DO GENDER DISTRIBUTION AND MEDIAN LOSS VARY BASED ON THE PERPETRATOR’S LEVEL OF AUTHORITY?



PERPETRATOR'S AGE

The age distribution of fraud perpetrators in our study resembles a bell curve with the majority of frauds (54%) having been committed by people between the ages of 31 and 45. Median losses, on the other hand, tended to directly correlate with age. Only 3% of fraudsters were over the age of 60, but the median loss in this group was USD 800,000, which far surpassed any other age category.

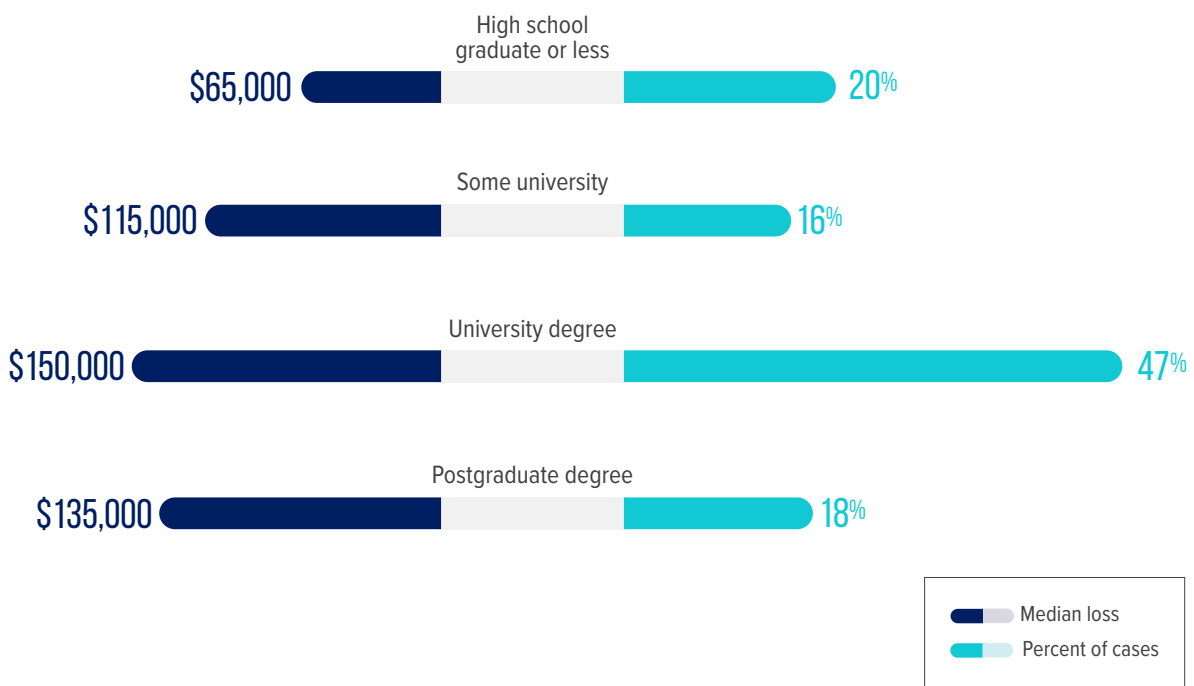
FIG. 39 HOW DOES THE PERPETRATOR'S AGE RELATE TO OCCUPATIONAL FRAUD?



PERPETRATOR'S EDUCATION LEVEL

As seen in Figure 40, 65% of occupational fraud perpetrators had a university degree or higher. Median losses were also larger among this group compared to those with lower education levels. Generally, we would expect losses to correlate to educational background because those with higher levels of authority also tend to have higher levels of education.

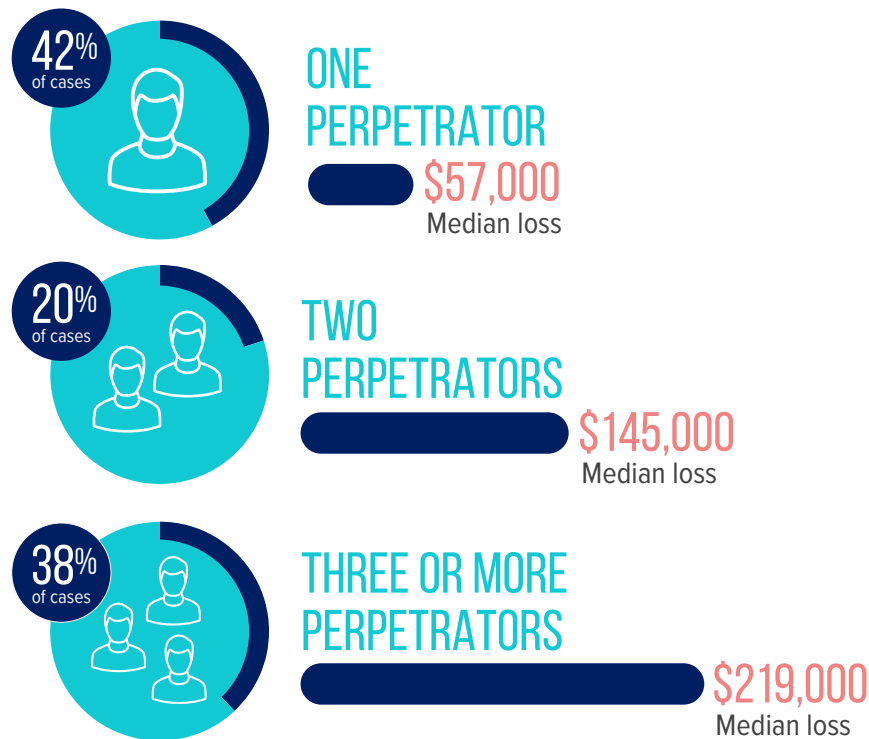
FIG. 40 HOW DOES THE PERPETRATOR'S EDUCATION LEVEL RELATE TO OCCUPATIONAL FRAUD?



COLLUSION BY MULTIPLE PERPETRATORS

The majority of frauds in our study (58%) were committed by two or more perpetrators acting in collusion. As Figure 41 illustrates, median losses tend to rise significantly when more than one person conspires to commit fraud. One likely reason for larger losses in collusive schemes is that multiple perpetrators working together may be able to circumvent controls based on separated duties and independent verification of transactions. Interestingly, however, the median duration of frauds in all three categories was the same (12 months), meaning frauds committed by multiple perpetrators tended to be caught just as quickly as frauds committed by single perpetrators.

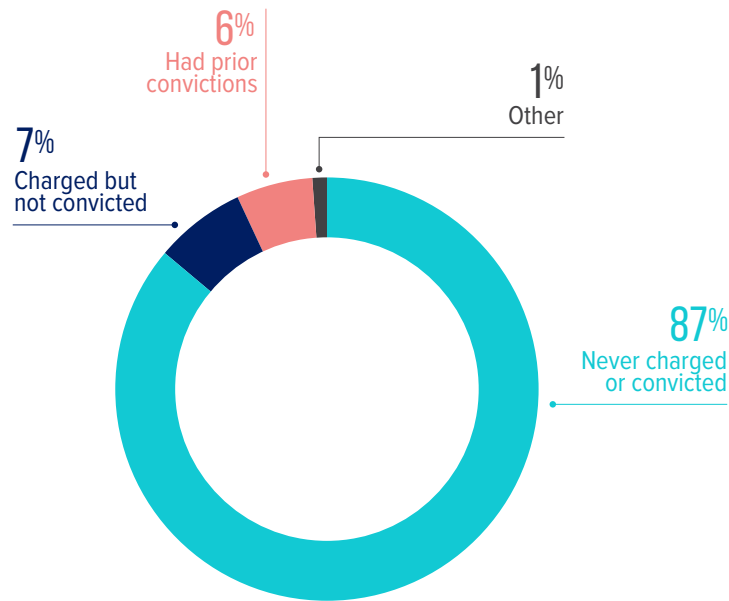
FIG. 41 HOW DOES THE NUMBER OF PERPETRATORS IN A SCHEME RELATE TO OCCUPATIONAL FRAUD?



PERPETRATOR'S CRIMINAL BACKGROUND

Only 6% of perpetrators in our study had a prior fraud-related conviction, which is consistent with our findings in previous studies. It is worth noting, however, that 42% of cases in our study were not reported to law enforcement (see Response to Fraud infographic, page 63), which is also consistent with prior findings. Because so many frauds go unreported, it is very likely that the true number of repeat offenders is higher than the 6% who have prior convictions.

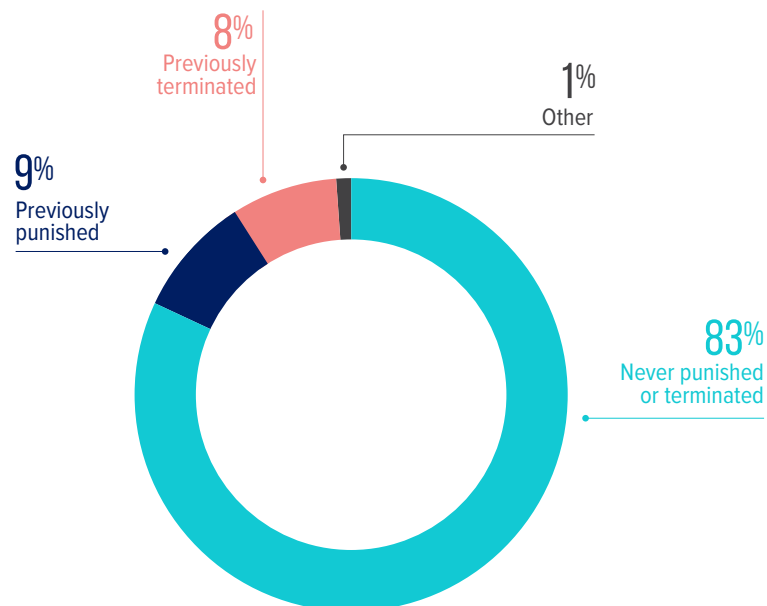
FIG. 42 DO PERPETRATORS TEND TO HAVE PRIOR FRAUD CONVICTIONS?



PERPETRATOR'S EMPLOYMENT HISTORY

As seen in Figure 43, 83% of fraudsters in our study had no prior record of having been punished or terminated by an employer for fraud-related conduct. But similar to the criminal conviction data in Figure 42, it is possible that this overstates the true number of first-time offenders. As seen in Figure 47 on page 62, 7% of fraudsters in our study were not punished, 11% were permitted to resign, and 10% signed settlement agreements with the victim organization. This indicates that a considerable number of fraudsters may have no employment disciplinary record for fraud even after having been caught.

FIG. 43 DO PERPETRATORS TEND TO HAVE PRIOR EMPLOYMENT-RELATED DISCIPLINARY ACTIONS FOR FRAUD?

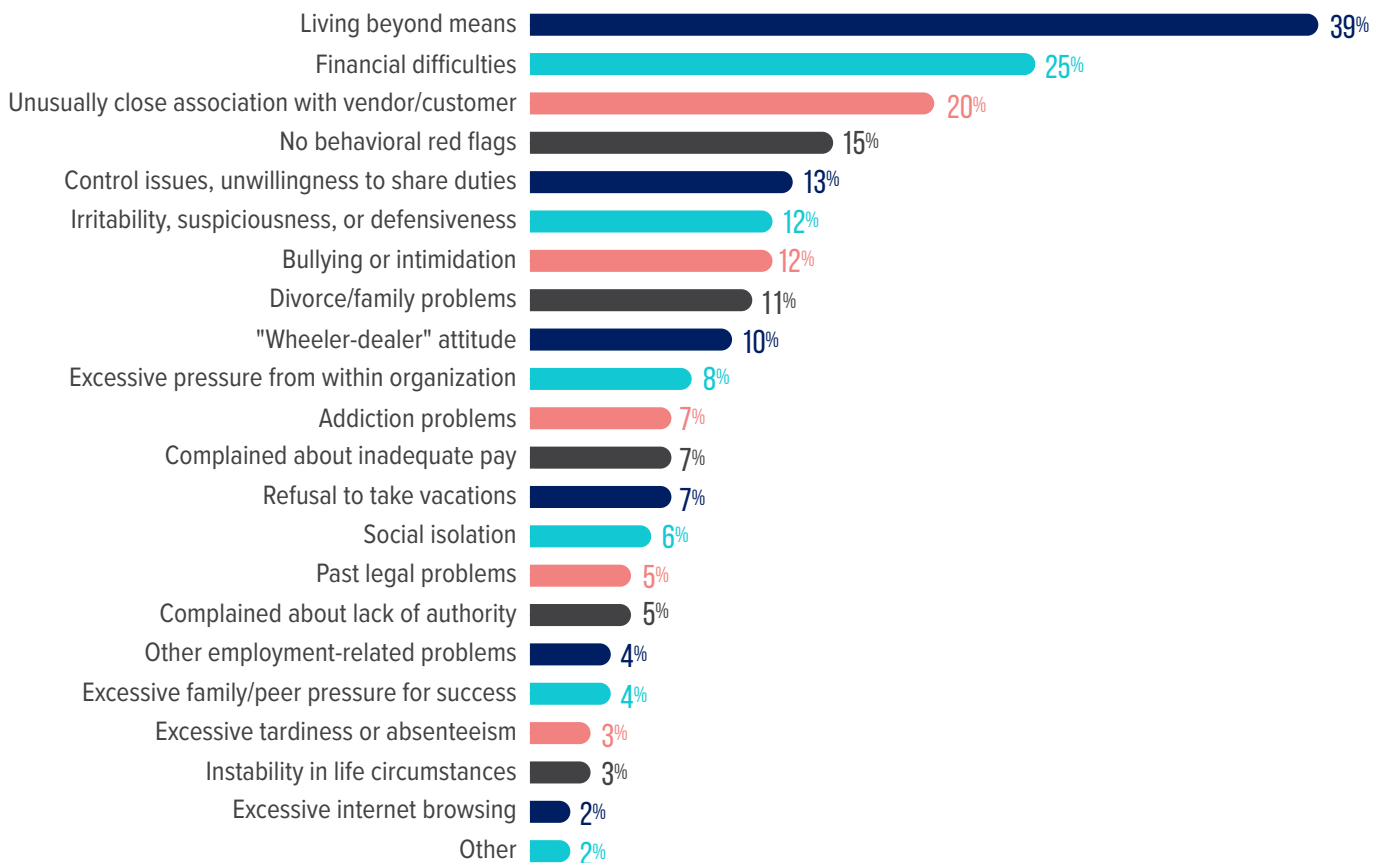


BEHAVIORAL RED FLAGS DISPLAYED BY PERPETRATORS

When a person is engaged in occupational fraud, that person will often display certain behavioral traits that tend to be associated with fraudulent conduct. The median duration of a fraud in our study was 12 months, which means that for a full year before the typical fraud is detected, the perpetrator may be exhibiting warning signs that could help the victim organization discover the crime.

We presented survey respondents with a list of 20 common behavioral red flags of fraud⁴, and asked which, if any, of these red flags were displayed by the perpetrator before the fraud was eventually detected. Figure 44 shows the results of this analysis. At least one red flag had been identified in 85% of the cases in our study, and multiple red flags were present in 51% of cases. The eight most common red flags were: (1) living beyond means; (2) financial difficulties; (3) unusually close association with a vendor or customer; (4) excessive control issues or unwillingness to share duties; (5) unusual irritability, suspiciousness, or defensiveness; (6) bullying or intimidation; (7) recent divorce or family problems; and (8) a general “wheeler-dealer” attitude involving shrewd or unscrupulous behavior. At least one of these eight red flags was identified in 76% of all cases.

FIG. 44 HOW OFTEN DO PERPETRATORS EXHIBIT BEHAVIORAL RED FLAGS?



⁴We added three new red flags to our survey this year that were not included in this question in previous studies: bullying or intimidation; excessive tardiness or absenteeism; and excessive internet browsing.

HUMAN RESOURCES—RELATED RED FLAGS

Figure 46 includes a list of factors that might relate to the fraudsters' job performance or job security as would likely be noted in human resources (HR) records. We refer to these as HR-related red flags. Each of these factors could potentially cause financial stress or resentment toward an employer, which might impact a person's decision to commit fraud. As shown in Figure 45, 50% of fraudsters had exhibited at least one HR-related red flag prior to or during the time of their frauds. The three most common were fear of job loss, poor performance evaluations, and having been denied a raise or promotion. Each of these flags was cited in more than 10% of all cases.

FIG. 45 DO FRAUD PERPETRATORS EXPERIENCE NEGATIVE HR-RELATED ISSUES PRIOR TO OR DURING THEIR FRAUDS?

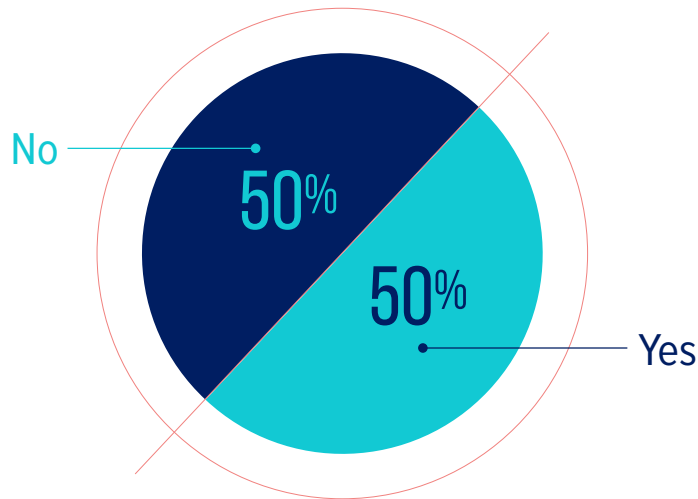
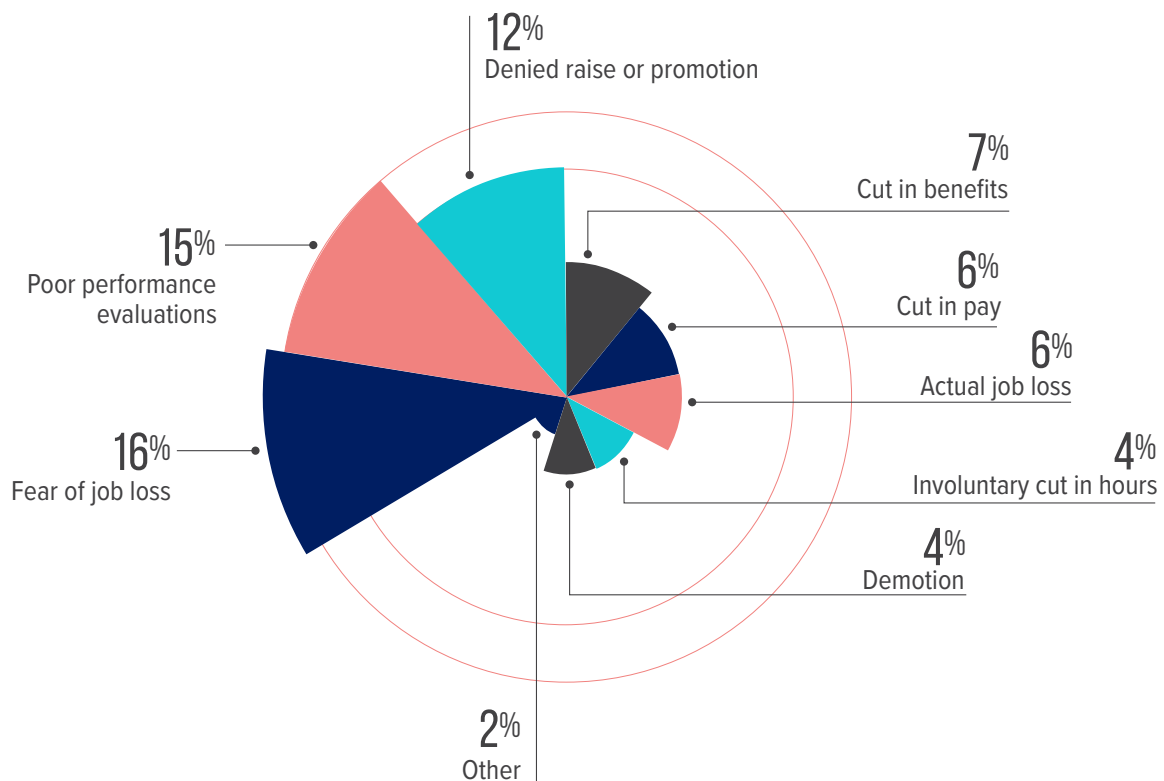


FIG. 46 WHICH HR-RELATED ISSUES ARE MOST COMMONLY EXPERIENCED BY FRAUD PERPETRATORS?



BEHAVIORAL RED FLAGS OF FRAUD

Recognizing the behavioral clues displayed by fraudsters can help organizations more effectively detect fraud and minimize their losses.

8 KEY WARNING SIGNS

85%

OF ALL FRAUDSTERS displayed at least one **BEHAVIORAL RED FLAG**

These are the 8 most common behavioral clues of occupational fraud. **At least one of these red flags** was observed in 76% of all cases.



39%

Living beyond means



25%

Financial difficulties



20%

Unusually close association with vendor/customer



13%

Control issues, unwillingness to share duties



12%

Irritability, suspiciousness, or defensiveness



12%

Bullying or intimidation



11%

Divorce/family problems



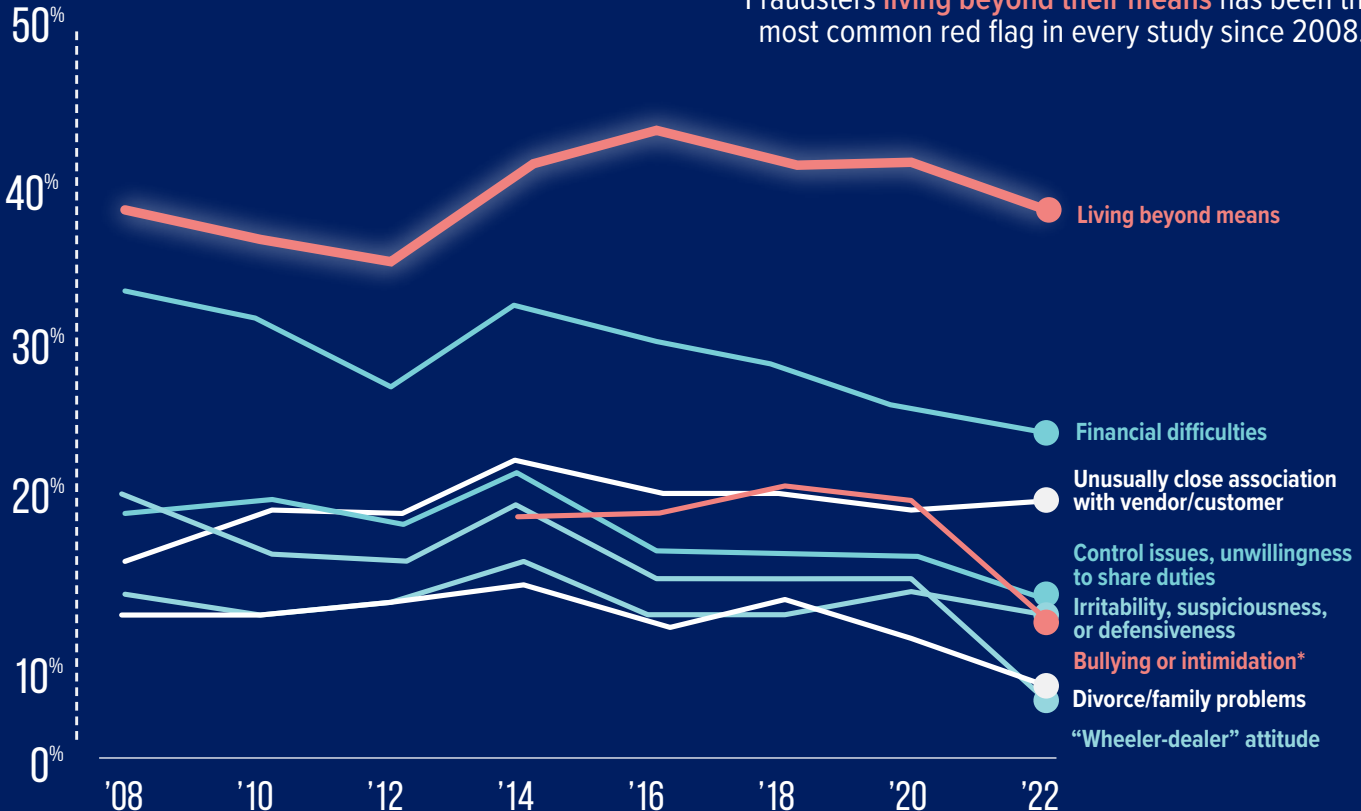
10%

"Wheeler-dealer" attitude

LIVING BEYOND MEANS



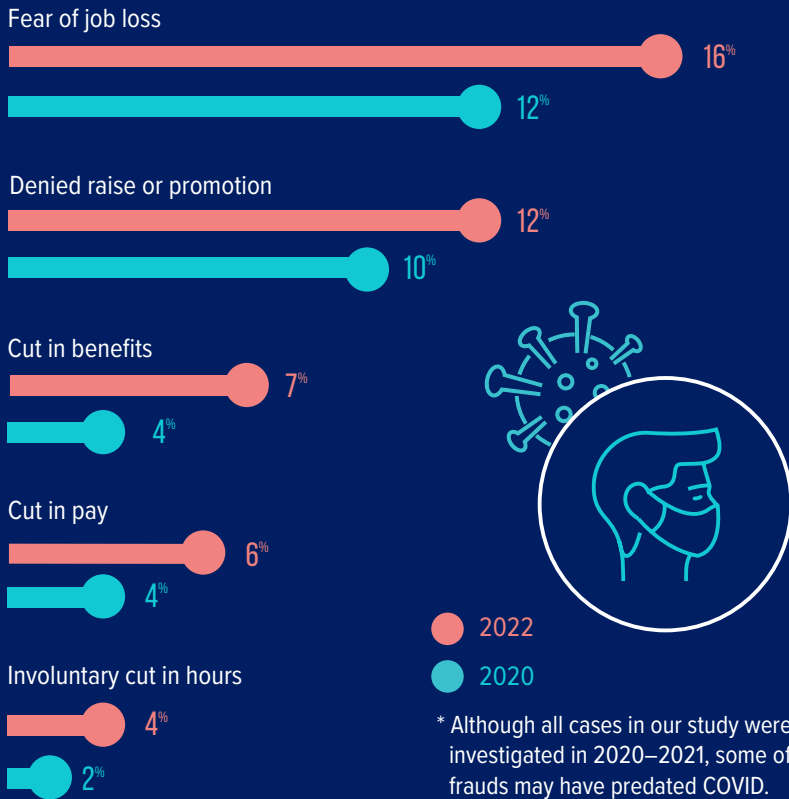
Fraudsters **living beyond their means** has been the most common red flag in every study since 2008.



* "Bullying or intimidation" was included as an option in our survey beginning in 2014 and was asked in a separate question prior to 2022.

DID JOB UNCERTAINTY DURING COVID CONTRIBUTE TO FRAUD?

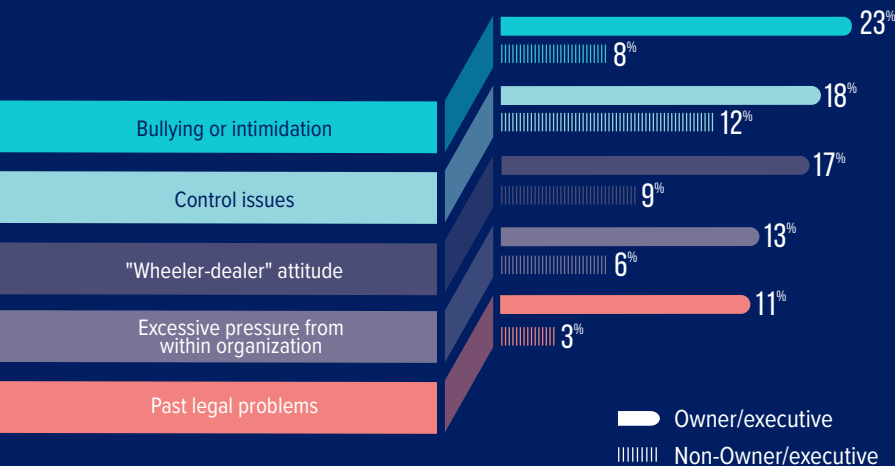
These five HR-related issues all involve a fraudster's job or compensation security. **All five increased in 2022.**



* Although all cases in our study were investigated in 2020–2021, some of the frauds may have predated COVID.

RED FLAGS IN THE C-SUITE

These **5 red flags** were much more common among owner/executives



GENDER AND RED FLAGS

Some behavioral flags tended to correlate with the fraudster's gender.



MORE COMMON WITH FEMALE FRAUDSTERS



Living beyond means

44%

37%



Financial difficulties

34%

22%



Recent divorce or family problems

17%

9%



MORE COMMON WITH MALE FRAUDSTERS



Unusually close association with vendor/customer

23%

13%



"Wheeler-dealer" attitude

13%

5%



Bullying or intimidation

13%

9%

CASE RESULTS



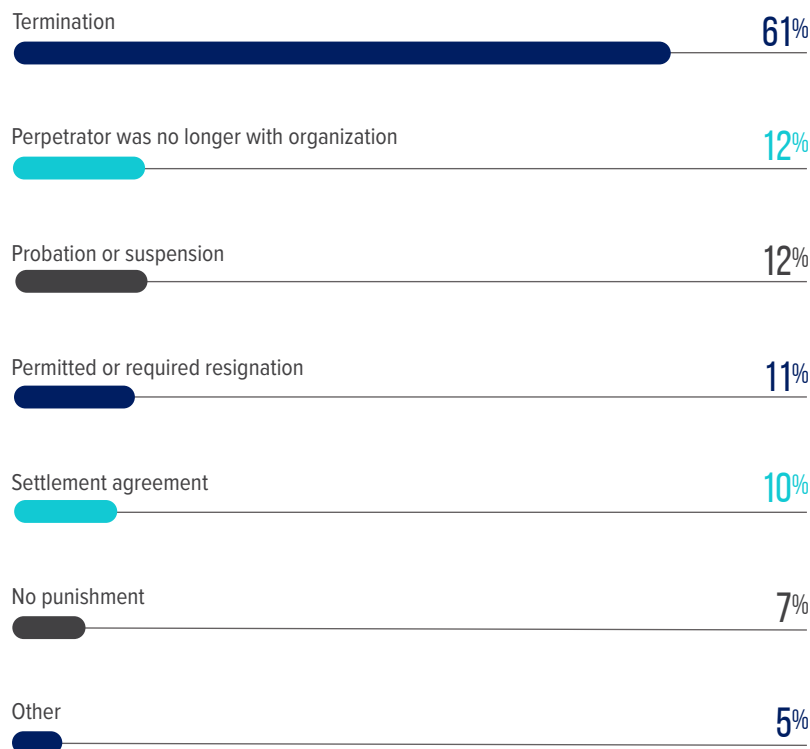
We asked survey participants how the victim organizations responded to the discovery of fraud and the outcome those responses produced. This information gives an idea of how organizations handle internal discipline of employees found to be committing fraud, the types of civil and criminal legal repercussions for fraudsters who faced litigation as a result of their actions, and the chances for recovering funds lost to fraud.



INTERNAL ACTION TAKEN AGAINST PERPETRATORS

Once an organization has identified fraud and determined who was responsible, it must decide whether to punish the perpetrator(s) and how. As in our previous studies, termination was by far the most common punishment faced by perpetrators (61% of cases). In 11% of cases, the perpetrator was permitted or required to resign in lieu of termination, and in 12% of cases, the perpetrator had already left the victim organization before the fraud was discovered.

FIG. 47 HOW DO VICTIM ORGANIZATIONS PUNISH FRAUD PERPETRATORS?



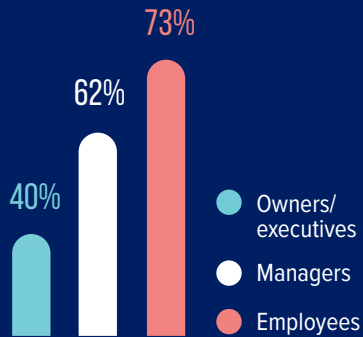
RESPONSE TO FRAUD

Outcomes in fraud cases vary based on the role of the perpetrator, the scheme carried out, the losses incurred, and how the organization responds.

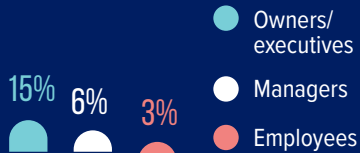
INTERNAL PUNISHMENT

Owners/executives are **LEAST LIKELY** to be punished for fraud

Termination for fraud



Received no punishment



Made a criminal referral **AND** filed a civil suit



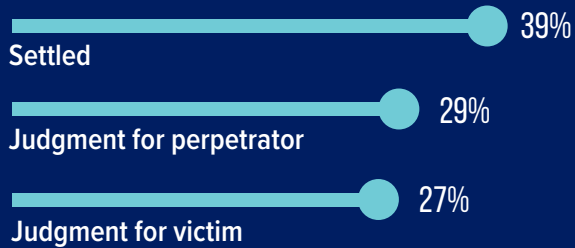
Did not make a criminal referral or file a civil suit



CIVIL LITIGATION

29% of cases resulted in **CIVIL LITIGATION**

MEDIAN LOSS in these cases: **\$300,000**

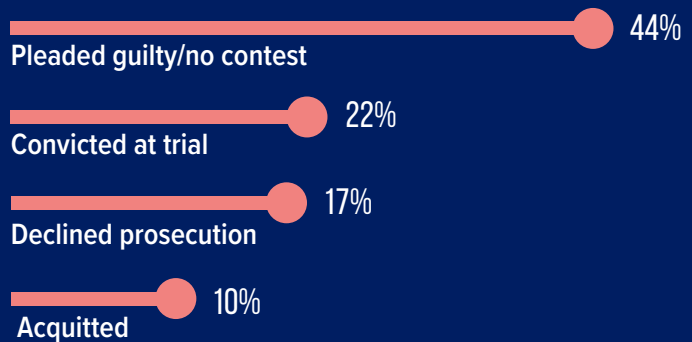


MEDIAN LOSS for those **THAT DECLINED** to file civil suits **\$70,000**

CRIMINAL REFERRALS

58% of cases resulted in **CRIMINAL REFERRAL**

MEDIAN LOSS in these cases: **\$200,000**



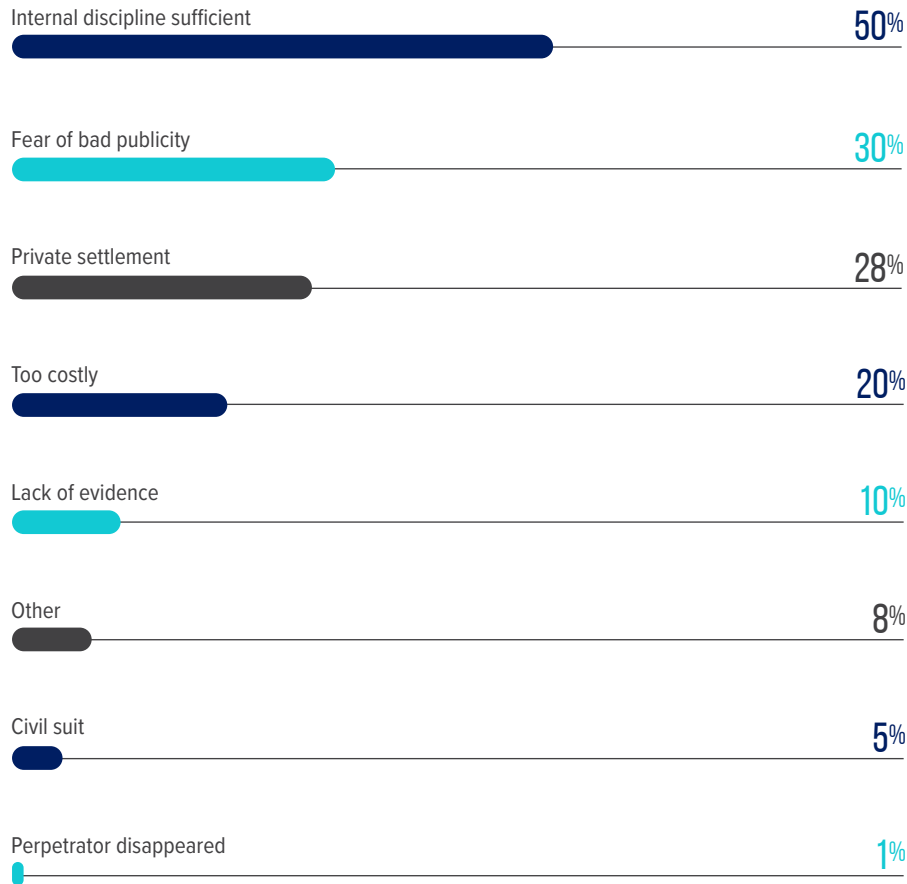
66% "SUCCESS RATE" of criminal referrals (perpetrator pleaded guilty + convicted)

LEAST likely to be referred to law enforcement
EXPENSE REIMBURSEMENT • NONCASH • BILLING/CORRUPTION

MEDIAN LOSS for those **THAT DECLINED** to refer **\$50,000**

As illustrated in the Response to Fraud infographic on page 63, not all fraud cases end up in civil or criminal courts. Moreover, not all cases that do involve litigation lead to negative consequences for fraudsters. To better understand organizations' rationales for not pursuing criminal charges against fraudsters, we asked respondents whose organizations did not refer their cases to law enforcement why they chose not to. Internal discipline being deemed sufficient was the most commonly cited reason (50%), with fear of bad publicity ranking second (30%), and private settlements third (28%).

FIG. 48 WHY DO ORGANIZATIONS DECLINE TO REFER CASES TO LAW ENFORCEMENT?



61%

of perpetrators were terminated by their employers



58%

of cases were referred to law enforcement



66%

of cases referred to law enforcement resulted in a conviction



50%

of organizations that didn't refer cases to law enforcement cited internal discipline as the reason

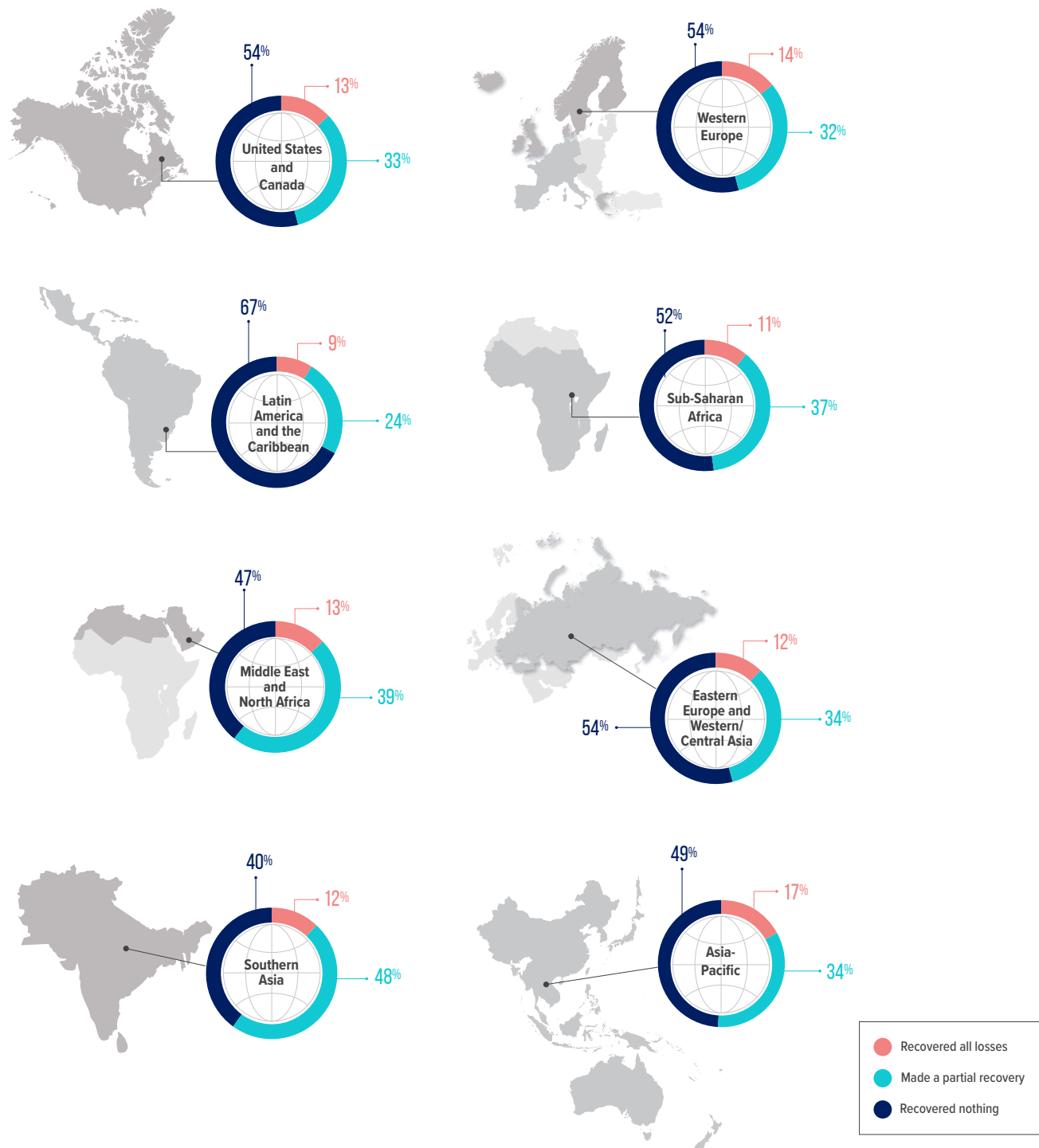
RECOVERING FRAUD LOSSES

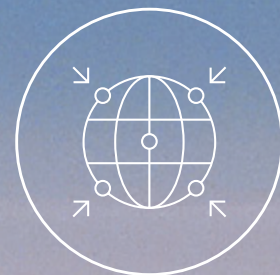
One of the primary motivating factors for management in determining an organization's response to fraud is the ability to recover funds and assets lost to the fraud. Unfortunately, in more than half of the cases in our study (52%), the victim organization did not recover any of its fraud losses. To determine whether the geographic location of the organization was correlated with success in recovering fraud losses, we analyzed the responses by region. Based on our findings, recovering fraud losses proved to be challenging worldwide. Only in the Middle East and North Africa (52%), Southern Asia (60%), and the Asia-Pacific (51%) regions were more than half of victim organizations able to recover any fraud losses. In every region, at least 40% of organizations recovered nothing.



52%
of victim organizations
DID NOT RECOVER
any fraud losses.

FIG. 49 HOW DID THE RECOVERY OF FRAUD LOSSES VARY BY REGION?





Occupational Fraud 2022: A Report to the Nations is based on the results of the ACFE 2021 *Global Fraud Survey*, an online survey opened to 53,118 Certified Fraud Examiners (CFEs) conducted from July 2021 to September 2021.

As part of the survey, respondents were asked to provide a narrative description of the single largest occupational fraud case they had investigated since January 2020. Respondents were then presented with questions regarding the details of the fraud case, including information about the perpetrator, the victim organization, and the methods of fraud employed, as well as fraud trends in general. (Respondents were not asked to identify the perpetrator or the victim.)

We received 7,890 total responses to the survey, 2,110 of which were usable for purposes of the report. The data contained herein is based solely on the information provided in these 2,110 survey responses.

CASES SUBMITTED WERE REQUIRED TO MEET THE FOLLOWING FOUR CRITERIA:

1. The case must have involved occupational fraud (i.e., fraud committed by a person against the organization for which they work).
2. The investigation must have occurred between January 2020 and the time of survey participation.
3. The investigation must have been complete at the time of survey participation.
4. The respondent must have been reasonably sure the perpetrator(s) was (were) identified.

ANALYSIS METHODOLOGY

PERCENTAGES

In calculating the percentages discussed throughout this report, we used the total number of complete and relevant responses for the question(s) being analyzed. Specifically, we excluded any blank responses or instances where the participant indicated that they did not know the answer to a question. Consequently, the total number of cases included in each analysis varies.

In addition, several survey questions allowed participants to select more than one answer. Therefore, the sum of percentages in many figures throughout the report exceeds 100%. The sum of percentages in other figures might not be exactly 100% (i.e., it might be 99% or 101%) due to rounding of individual category data.

LOSS AMOUNTS

All loss amounts are expressed in terms of U.S. dollars, which is how respondents reported this information in the *Global Fraud Survey*.

Unless otherwise indicated, all loss amounts discussed throughout the report are calculated using median loss rather than mean, or average, loss. Using median loss provides a more conservative—and we believe more accurate—picture of the typical impact of occupational fraud schemes. The statistical appendix to this report (see pages 86–88) provides a more holistic view of the losses in our study, reflecting quartiles and average loss amounts for numerous categories explored throughout the report.

To normalize the loss amounts reported to us and ensure that cases with extremely large losses were not identifiable, all average and total loss amounts reported were calculated using loss data that was winsorized at 5% (i.e., all cases in the top 2.5% and bottom 2.5% were assigned the same value as the 97.5th percentile and 2.5th percentile, respectively). Additionally, we excluded median and average loss calculations for categories for which there were fewer than ten responses.

Because the direct losses caused by financial statement frauds are typically spread among numerous stakeholders, obtaining an accurate estimate for this amount is extremely difficult. Consequently, for schemes involving financial statement fraud, we asked survey participants to provide the gross amount of the financial statement misstatement (over- or understatement) involved in the scheme. All losses reported for financial statement frauds throughout this report are based on those reported amounts.

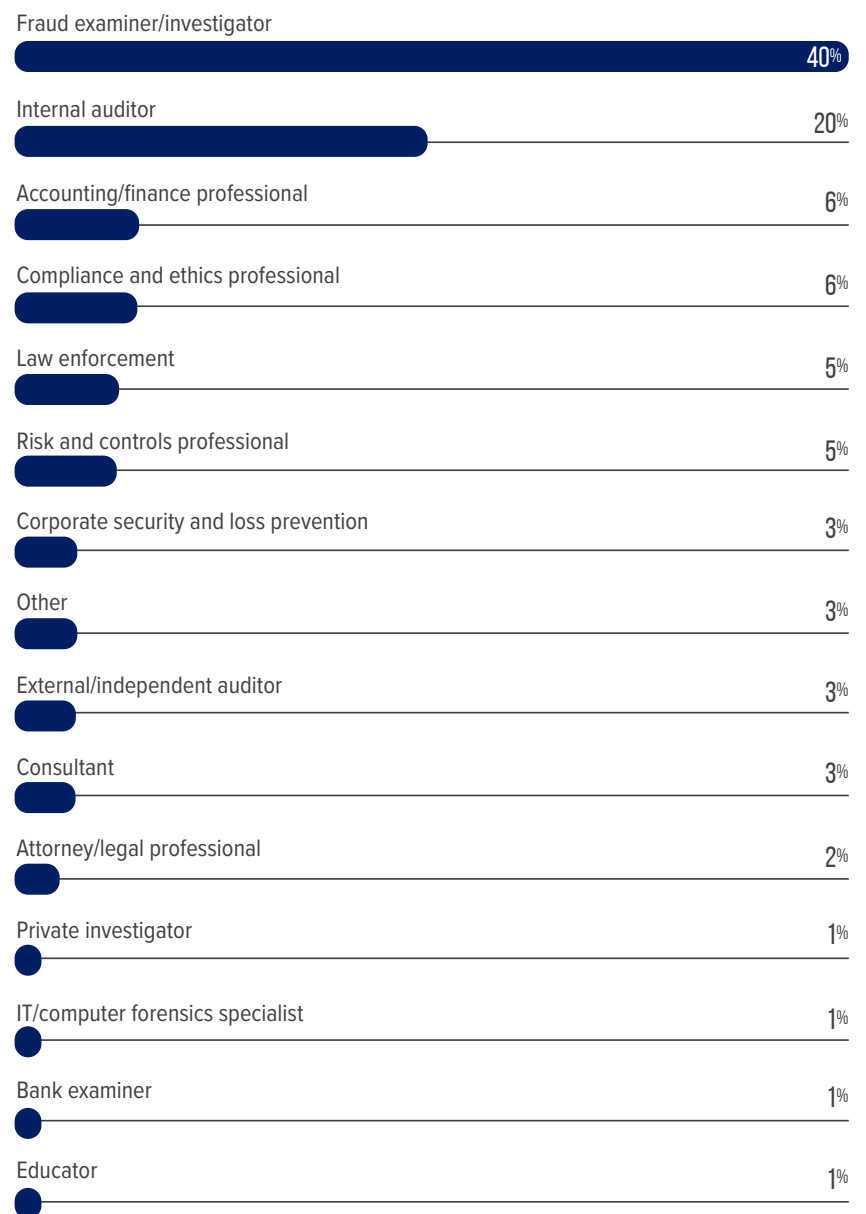
SURVEY PARTICIPANTS

To provide context for the survey responses and to understand who investigates cases of occupational fraud, we asked respondents to provide certain information about their professional experience and qualifications.

PRIMARY OCCUPATION

The majority of survey respondents indicated that their primary profession is either a fraud examiner/investigator (40%) or an internal auditor (20%).

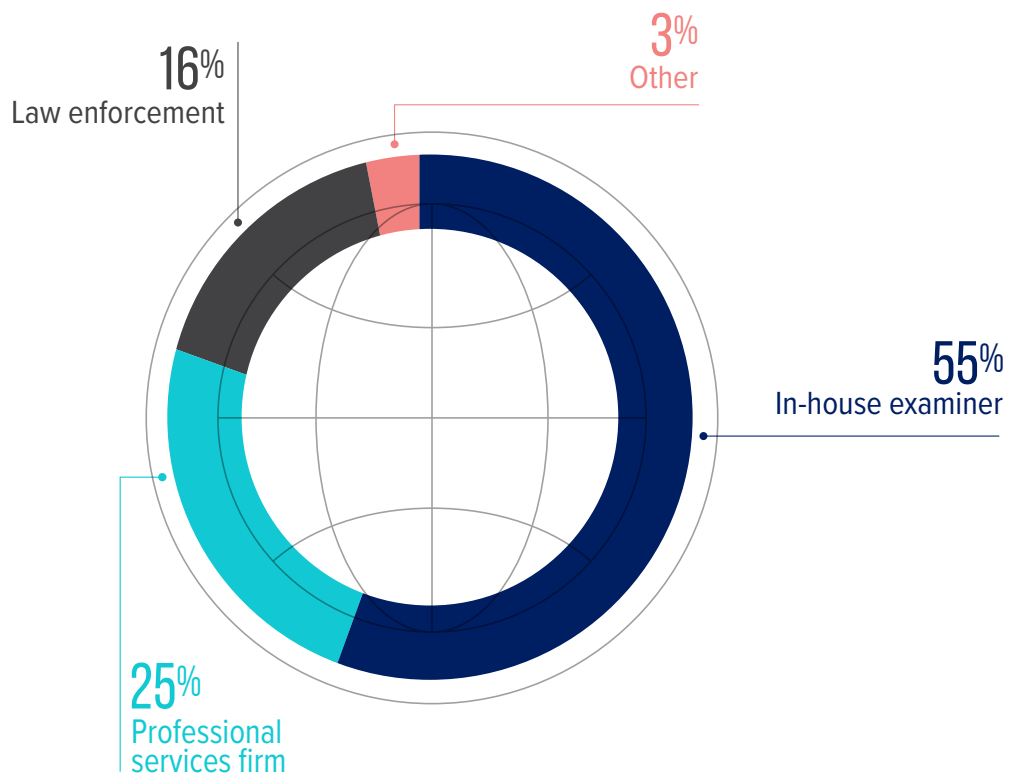
FIG. 50 WHAT WAS THE PRIMARY OCCUPATION OF SURVEY PARTICIPANTS?



NATURE OF FRAUD EXAMINATION ROLE

More than half of our survey participants (55%) work in-house and conduct fraud-related engagements on behalf of a single organization (i.e., their employer), while one-quarter work for a professional services firm that conducts fraud-related engagements for client organizations. In addition, 16% work for law enforcement agencies and conduct fraud investigations of other parties under their agency's authority.

FIG. 51 WHAT WAS THE PROFESSIONAL ROLE OF THE SURVEY PARTICIPANTS?



PROFESSIONAL EXPERIENCE

The CFEs who participated in the *Global Fraud Survey* had a median 11 years' experience in the fraud examination field, with 31% having more than 15 years of experience. Additionally, nearly one-quarter of participants have investigated more than 20 cases of fraud in the past two years (see Figure 53).

FIG. 52 HOW MUCH FRAUD EXAMINATION EXPERIENCE DID SURVEY PARTICIPANTS HAVE?

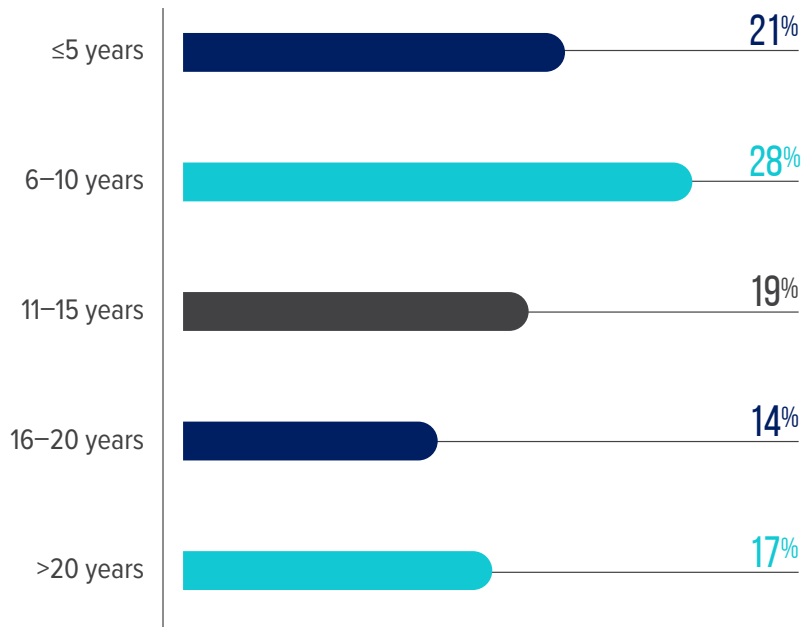
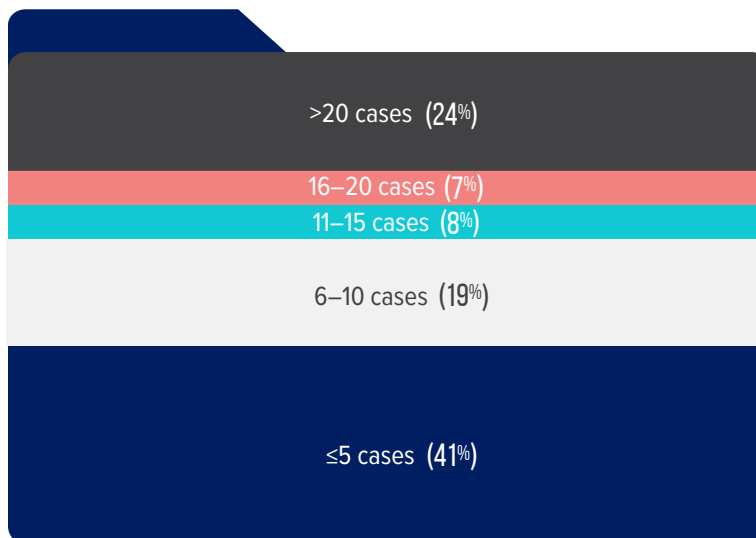


FIG. 53 HOW MANY FRAUD CASES HAVE SURVEY PARTICIPANTS INVESTIGATED IN THE PAST TWO YEARS?



REGIONAL FOCUS

ASIA-PACIFIC



FIG. 54 WHAT ARE THE MOST COMMON OCCUPATIONAL FRAUD SCHEMES IN THE ASIA-PACIFIC REGION?

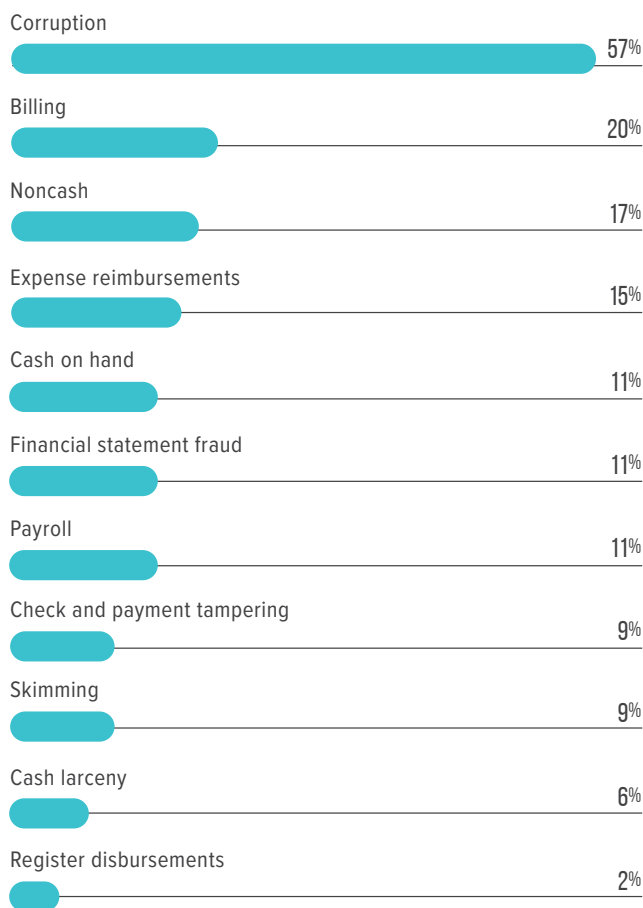


FIG. 55 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED IN THE ASIA-PACIFIC REGION?

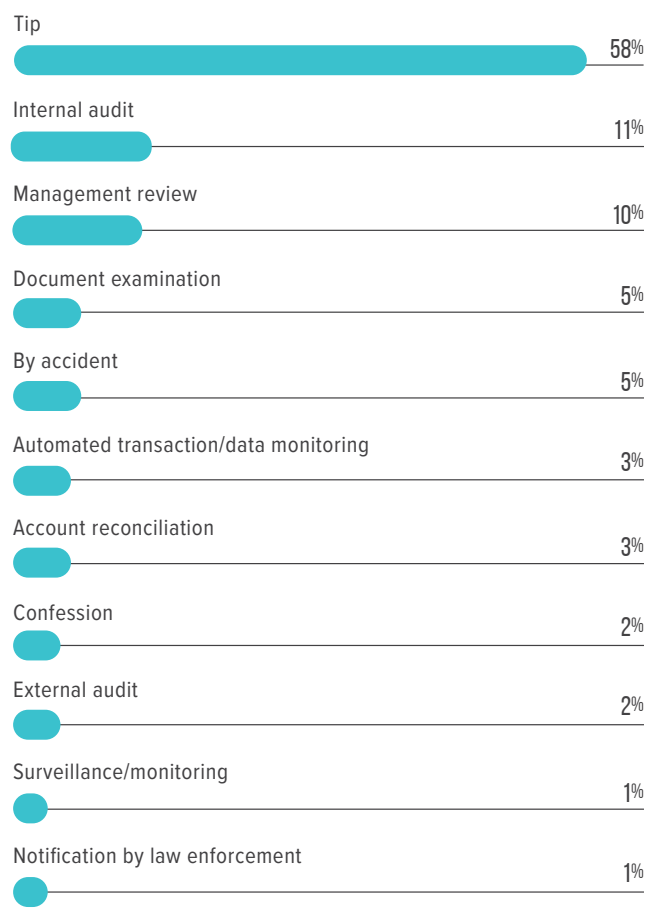


FIG. 56 WHAT ANTI-FRAUD CONTROLS ARE THE MOST COMMON IN THE ASIA-PACIFIC REGION?

Control	Percent of cases
External audit of financial statements	88%
Code of conduct	84%
Internal audit department	82%
Hotline	80%
Management certification of financial statements	77%
Fraud training for employees	76%
Independent audit committee	75%
Management review	75%
External audit of internal controls over financial reporting	73%
Anti-fraud policy	72%
Fraud training for managers/executives	69%
Employee support programs	59%
Dedicated fraud department, function, or team	55%
Formal fraud risk assessments	54%
Proactive data monitoring/analysis	52%
Surprise audits	46%
Job rotation/mandatory vacation	31%
Rewards for whistleblowers	14%

FIG. 57 HOW DOES THE PERPETRATOR'S LEVEL OF AUTHORITY RELATE TO OCCUPATIONAL FRAUD IN THE ASIA-PACIFIC REGION?

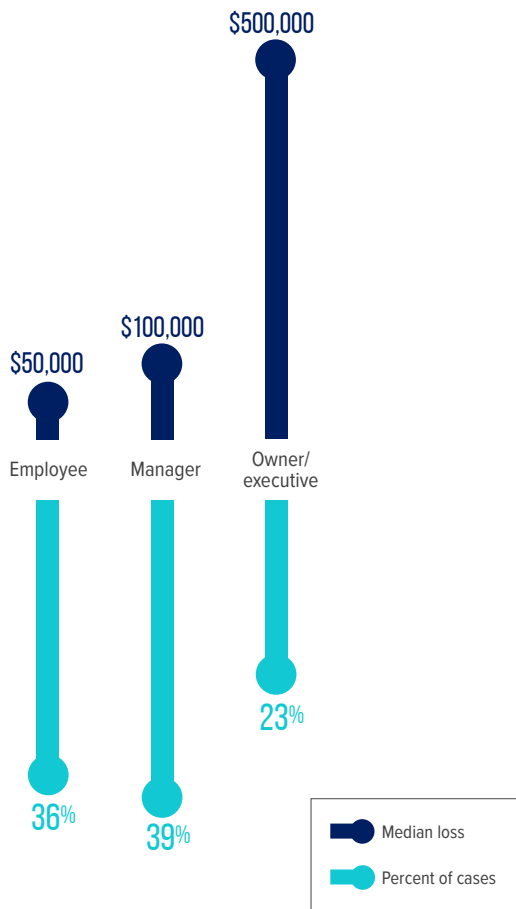
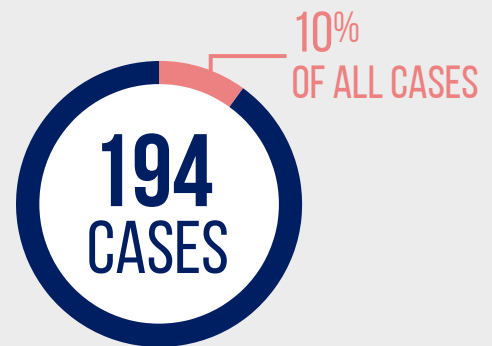


FIG. 58 CASES BY COUNTRY IN THE ASIA-PACIFIC REGION

Country	Number of cases
American Samoa	2
Australia	38
China	33
Fiji	1
Hong Kong	13
Indonesia	23
Laos	1
Malaysia	25
Micronesia	1
New Zealand	6
Papua New Guinea	3
Philippines	12
Singapore	13
Solomon Islands	1
South Korea	2
Taiwan	3
Thailand	9
Vietnam	8
TOTAL CASES	194

MEDIAN LOSS:
USD 121,000



EASTERN EUROPE AND WESTERN/CENTRAL ASIA



FIG. 59 WHAT ARE THE MOST COMMON OCCUPATIONAL FRAUD SCHEMES IN EASTERN EUROPE AND WESTERN/CENTRAL ASIA?

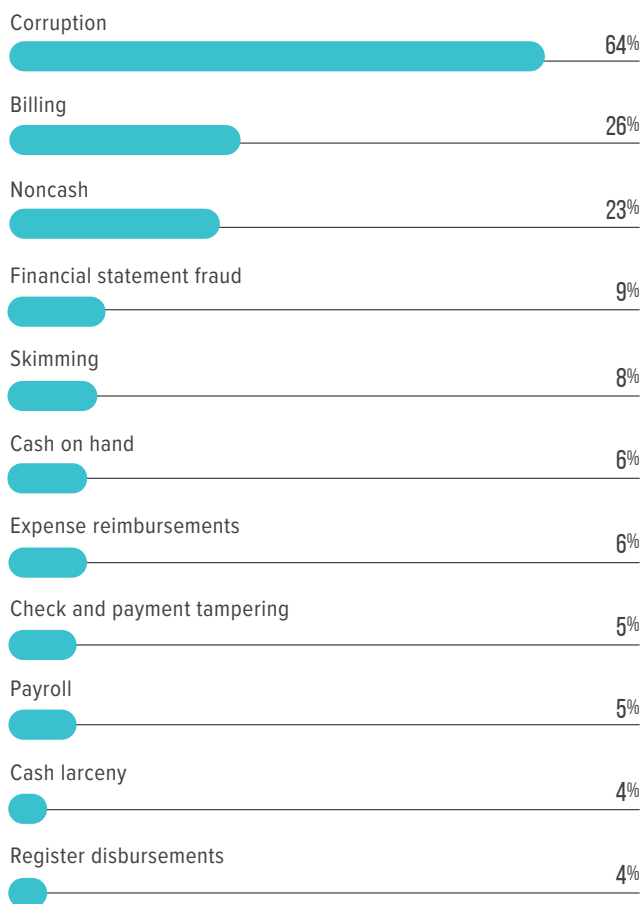


FIG. 60 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED IN EASTERN EUROPE AND WESTERN/CENTRAL ASIA?

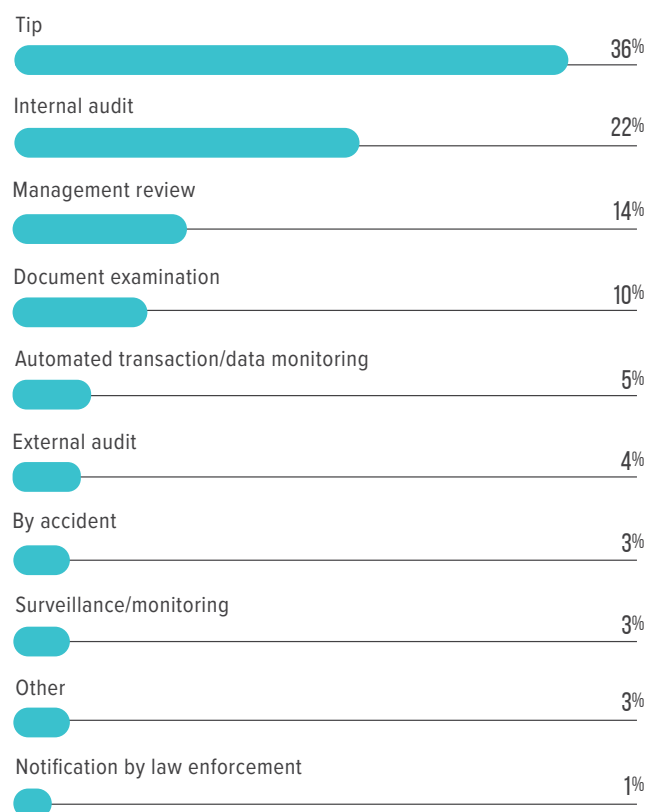


FIG. 61 WHAT ANTI-FRAUD CONTROLS ARE THE MOST COMMON IN EASTERN EUROPE AND WESTERN/CENTRAL ASIA?

Control	Percent of cases
Code of conduct	83%
External audit of financial statements	83%
Internal audit department	81%
Hotline	75%
Management review	71%
Independent audit committee	69%
Management certification of financial statements	68%
External audit of internal controls over financial reporting	66%
Fraud training for employees	62%
Fraud training for managers/executives	60%
Dedicated fraud department, function, or team	55%
Anti-fraud policy	52%
Surprise audits	46%
Proactive data monitoring/analysis	40%
Formal fraud risk assessments	37%
Employee support programs	21%
Job rotation/mandatory vacation	21%
Rewards for whistleblowers	12%

FIG. 62 HOW DOES THE PERPETRATOR'S LEVEL OF AUTHORITY RELATE TO OCCUPATIONAL FRAUD IN EASTERN EUROPE AND WESTERN/CENTRAL ASIA?

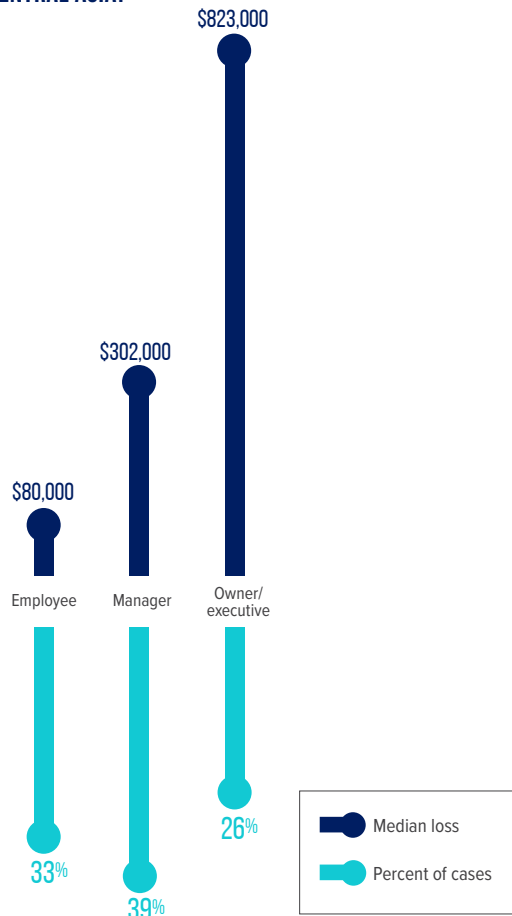
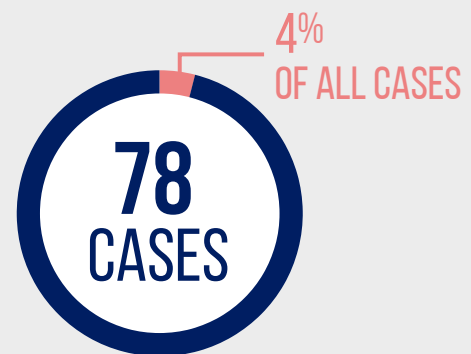


FIG. 63 CASES BY COUNTRY IN EASTERN EUROPE AND WESTERN/CENTRAL ASIA

Country	Number of cases
Albania	3
Azerbaijan	3
Bulgaria	5
Croatia	1
Czech Republic	8
Estonia	1
Hungary	1
Kazakhstan	2
Moldova	1
Poland	9
Romania	4
Russia	11
Serbia	6
Slovakia	2
Slovenia	1
Tajikistan	1
Turkey	8
Ukraine	11
TOTAL CASES	78

MEDIAN LOSS:
USD 190,000



REGIONAL FOCUS

LATIN AMERICA AND THE CARIBBEAN



FIG. 64 WHAT ARE THE MOST COMMON OCCUPATIONAL FRAUD SCHEMES IN LATIN AMERICA AND THE CARIBBEAN?

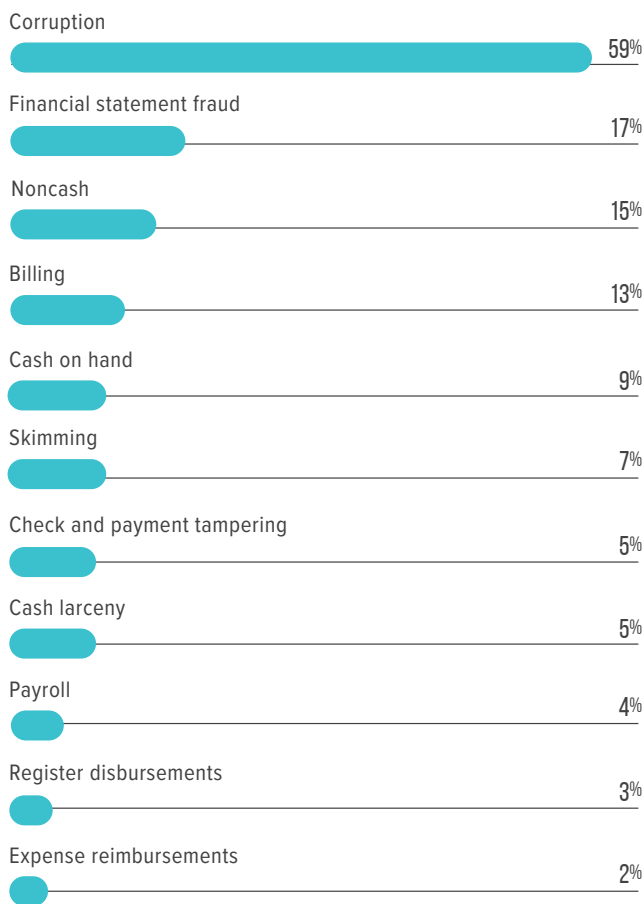


FIG. 65 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED IN LATIN AMERICA AND THE CARIBBEAN?

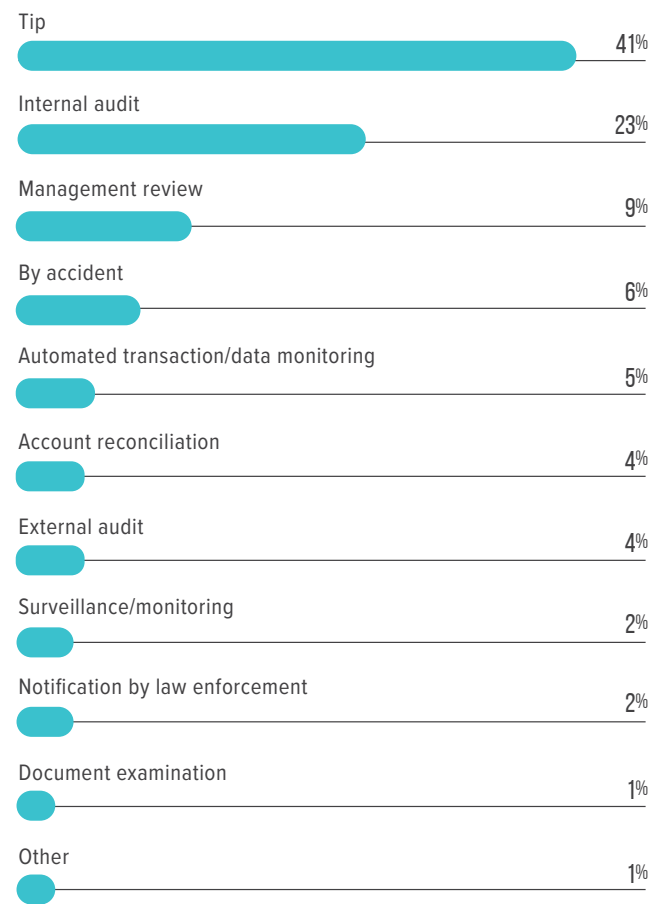


FIG. 66 WHAT ANTI-FRAUD CONTROLS ARE THE MOST COMMON IN LATIN AMERICA AND THE CARIBBEAN?

Control	Percent of cases
Code of conduct	84%
Internal audit department	81%
External audit of financial statements	76%
Management review	70%
Management certification of financial statements	69%
Independent audit committee	69%
Hotline	67%
External audit of internal controls over financial reporting	65%
Fraud training for managers/executives	52%
Anti-fraud policy	52%
Fraud training for employees	52%
Employee support programs	50%
Dedicated fraud department, function, or team	35%
Formal fraud risk assessments	32%
Proactive data monitoring/analysis	30%
Surprise audits	28%
Job rotation/mandatory vacation	21%
Rewards for whistleblowers	5%

FIG. 67 HOW DOES THE PERPETRATOR'S LEVEL OF AUTHORITY RELATE TO OCCUPATIONAL FRAUD IN LATIN AMERICA AND THE CARIBBEAN?

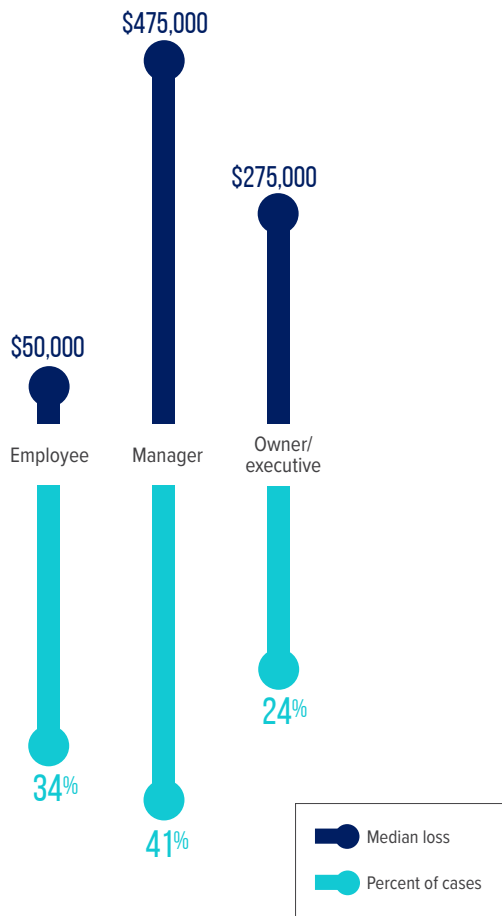
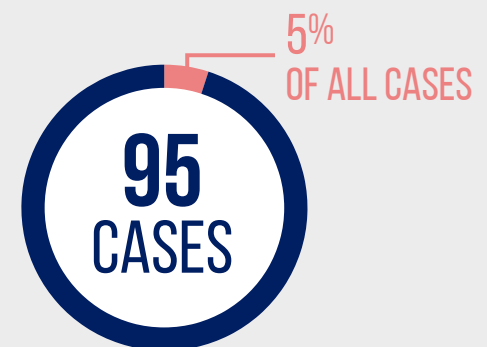


FIG. 68 CASES BY COUNTRY IN LATIN AMERICA AND THE CARIBBEAN

Country	Number of cases
Antigua and Barbuda	2
Argentina	8
Aruba	5
Bahamas	1
Barbados	2
Belize	2
Bermuda	1
Brazil	12
Chile	4
Colombia	7
Costa Rica	4
Curaçao	1
Guyana	1
Haiti	1
Jamaica	7
Mexico	22
Nicaragua	1
Panama	1
Peru	5
Suriname	2
Trinidad and Tobago	4
Uruguay	1
Virgin Islands, British	1
TOTAL CASES	95

MEDIAN LOSS:
USD 175,000



MIDDLE EAST AND NORTH AFRICA



FIG. 69 WHAT ARE THE MOST COMMON OCCUPATIONAL FRAUD SCHEMES IN THE MIDDLE EAST AND NORTH AFRICA?

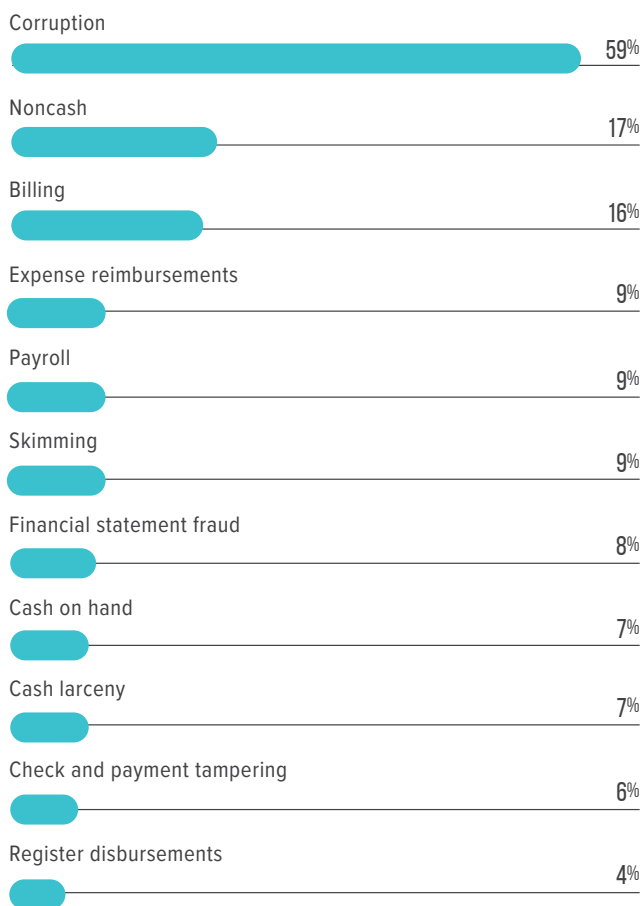


FIG. 70 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED IN THE MIDDLE EAST AND NORTH AFRICA?

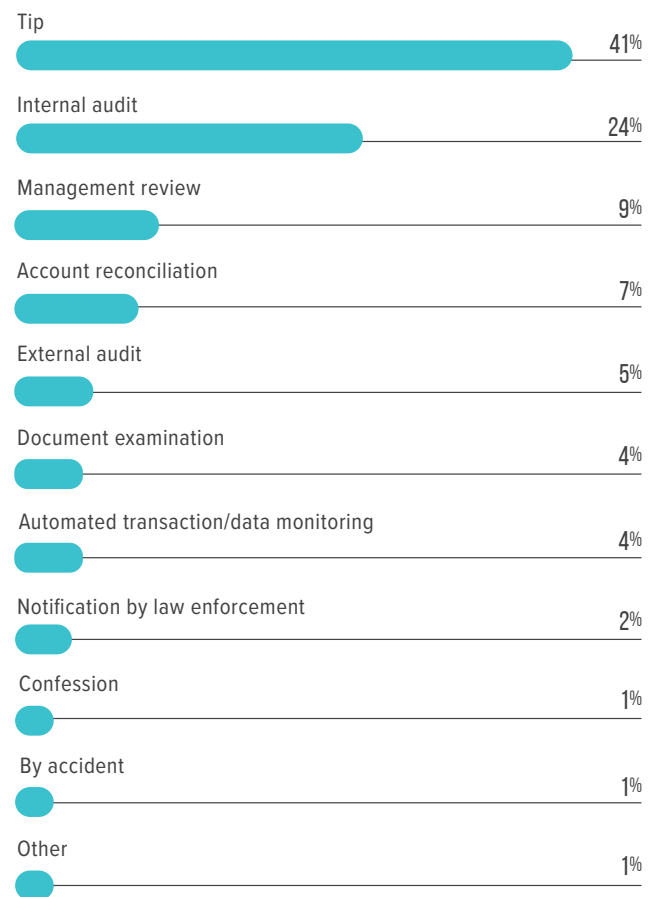


FIG. 71 WHAT ANTI-FRAUD CONTROLS ARE THE MOST COMMON IN THE MIDDLE EAST AND NORTH AFRICA?

Control	Percent of cases
External audit of financial statements	89%
Internal audit department	86%
Code of conduct	82%
Management certification of financial statements	79%
Management review	71%
Independent audit committee	71%
External audit of internal controls over financial reporting	70%
Hotline	68%
Anti-fraud policy	60%
Fraud training for employees	58%
Fraud training for managers/executives	54%
Surprise audits	48%
Dedicated fraud department, function, or team	44%
Formal fraud risk assessments	43%
Proactive data monitoring/analysis	43%
Employee support programs	32%
Job rotation/mandatory vacation	24%
Rewards for whistleblowers	14%

FIG. 72 HOW DOES THE PERPETRATOR'S LEVEL OF AUTHORITY RELATE TO OCCUPATIONAL FRAUD IN THE MIDDLE EAST AND NORTH AFRICA?

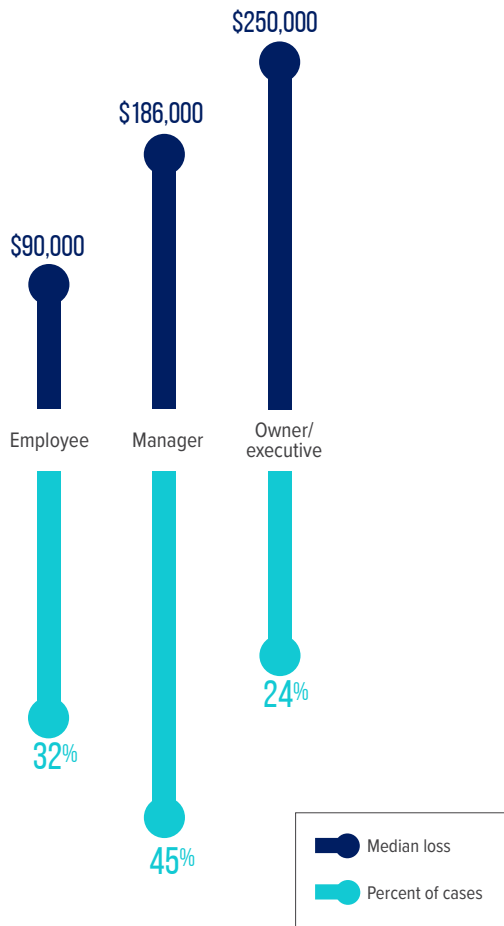
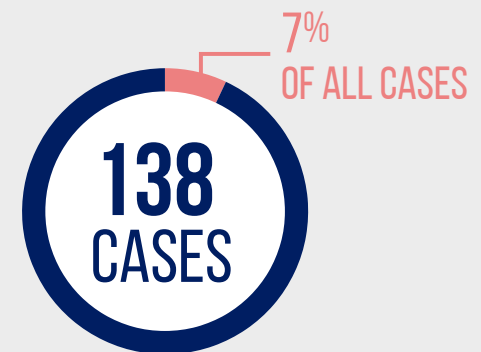


FIG. 73 CASES BY COUNTRY IN THE MIDDLE EAST AND NORTH AFRICA

Country	Number of cases
Algeria	1
Bahrain	3
Cyprus	4
Egypt	8
Iraq	1
Jordan	4
Kuwait	8
Lebanon	3
Malta	2
Oman	4
Qatar	7
Saudi Arabia	29
Tunisia	2
United Arab Emirates	60
Yemen	2
TOTAL CASES	138

MEDIAN LOSS:
USD 186,000



REGIONAL FOCUS

SOUTHERN ASIA



FIG. 74 WHAT ARE THE MOST COMMON OCCUPATIONAL FRAUD SCHEMES IN SOUTHERN ASIA?

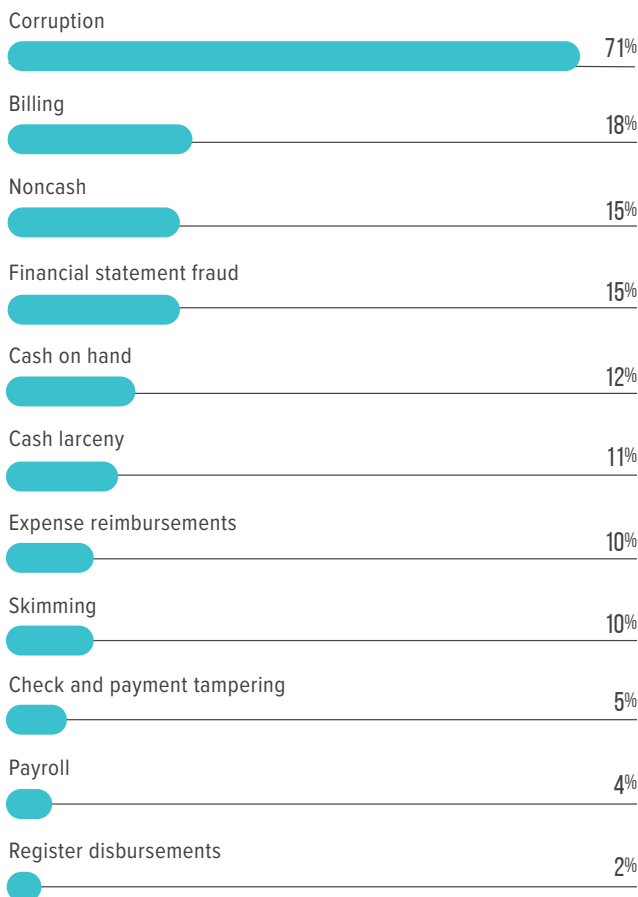


FIG. 75 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED IN SOUTHERN ASIA?



FIG. 76 WHAT ANTI-FRAUD CONTROLS ARE THE MOST COMMON IN SOUTHERN ASIA?

Control	Percent of cases
External audit of financial statements	91%
Code of conduct	88%
Internal audit department	85%
External audit of internal controls over financial reporting	85%
Management certification of financial statements	84%
Independent audit committee	76%
Management review	72%
Hotline	72%
Fraud training for managers/executives	66%
Fraud training for employees	63%
Anti-fraud policy	63%
Dedicated fraud department, function, or team	53%
Surprise audits	48%
Employee support programs	45%
Formal fraud risk assessments	45%
Proactive data monitoring/analysis	42%
Job rotation/mandatory vacation	33%
Rewards for whistleblowers	24%

FIG. 77 HOW DOES THE PERPETRATOR'S LEVEL OF AUTHORITY RELATE TO OCCUPATIONAL FRAUD IN SOUTHERN ASIA?

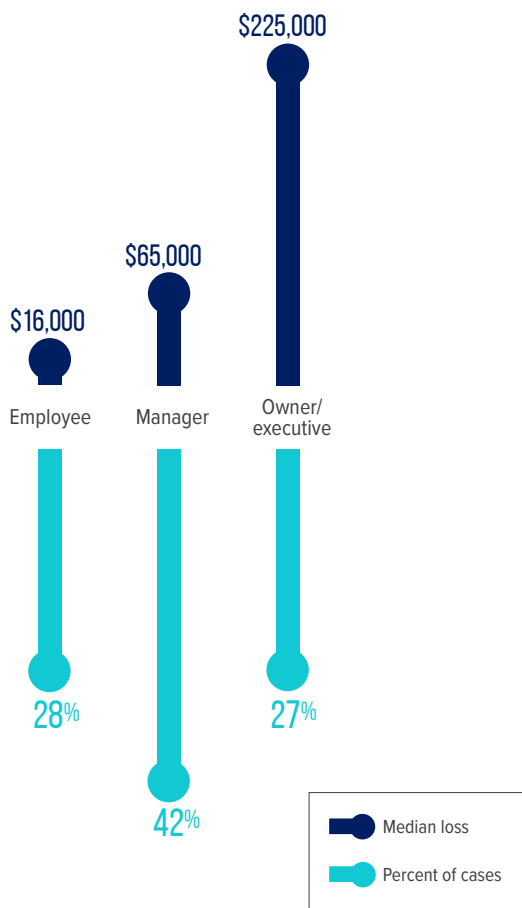
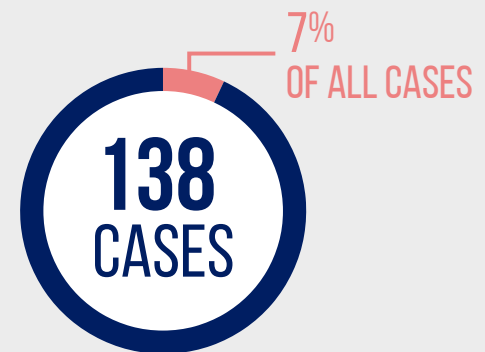


FIG. 78 CASES BY COUNTRY IN SOUTHERN ASIA

Country	Number of cases
Afghanistan	7
Bangladesh	7
Bhutan	1
India	103
Nepal	1
Pakistan	10
Sri Lanka	9
TOTAL CASES	138

MEDIAN LOSS:
USD 92,000



SUB-SAHARAN AFRICA



FIG. 79 WHAT ARE THE MOST COMMON OCCUPATIONAL FRAUD SCHEMES IN SUB-SAHARAN AFRICA?

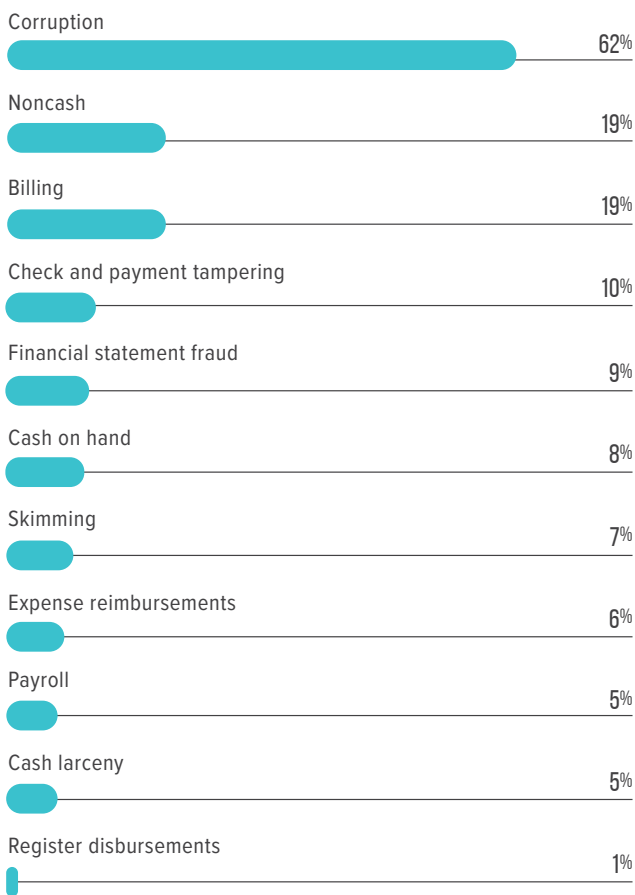


FIG. 80 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED IN SUB-SAHARAN AFRICA?

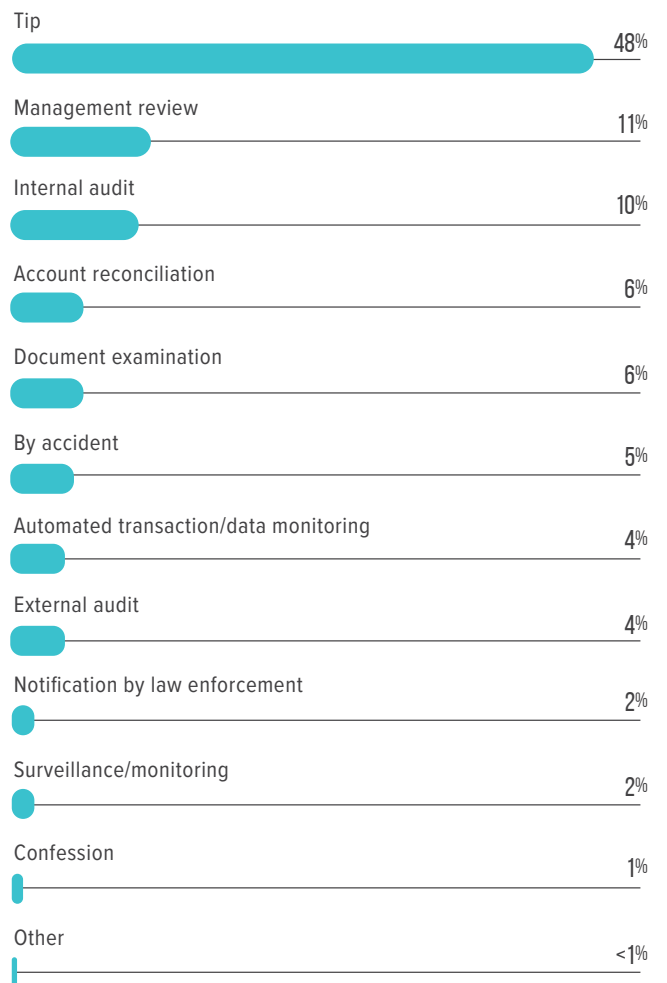


FIG. 81 WHAT ANTI-FRAUD CONTROLS ARE THE MOST COMMON IN SUB-SAHARAN AFRICA?

Control	Percent of cases
Code of conduct	89%
External audit of financial statements	87%
Internal audit department	87%
Management certification of financial statements	83%
Hotline	76%
External audit of internal controls over financial reporting	76%
Independent audit committee	74%
Management review	72%
Anti-fraud policy	69%
Fraud training for employees	67%
Fraud training for managers/executives	62%
Employee support programs	58%
Dedicated fraud department, function, or team	56%
Formal fraud risk assessments	53%
Proactive data monitoring/analysis	47%
Surprise audits	47%
Job rotation/mandatory vacation	30%
Rewards for whistleblowers	18%

FIG. 82 HOW DOES THE PERPETRATOR'S LEVEL OF AUTHORITY RELATE TO OCCUPATIONAL FRAUD IN SUB-SAHARAN AFRICA?

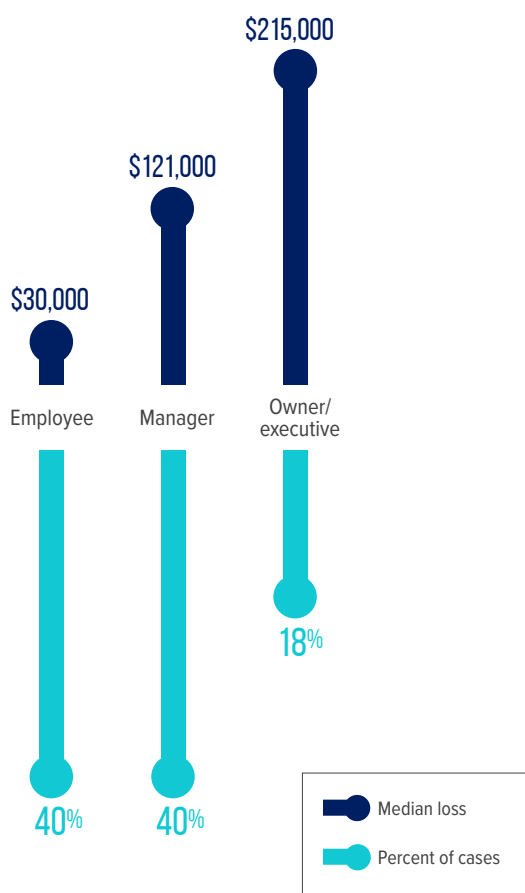
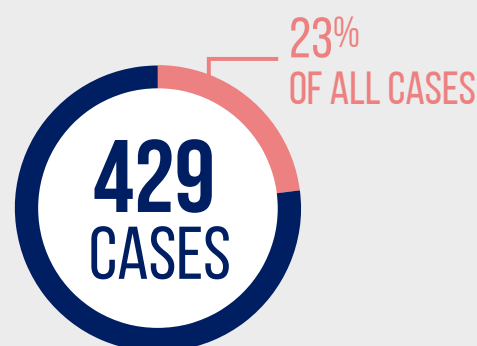


FIG. 83 CASES BY COUNTRY IN SUB-SAHARAN AFRICA

Country	Number of cases
Angola	2
Botswana	5
Burkina Faso	1
Burundi	2
Cameroon	4
Democratic Republic of the Congo	11
Ethiopia	1
Ghana	15
Kenya	49
Lesotho	5
Liberia	4
Madagascar	4
Malawi	9
Mali	1
Mauritius	5
Mozambique	2
Namibia	3
Niger	1
Nigeria	61
Rwanda	2
Senegal	3
Seychelles	1
Sierra Leone	2
Somalia	4
South Africa	188
South Sudan	1
Sudan	1
Swaziland	1
Tanzania	8
Togo	1
Uganda	16
Zambia	5
Zimbabwe	11
TOTAL CASES	429

MEDIAN LOSS:
USD 100,000



REGIONAL FOCUS

UNITED STATES AND CANADA



FIG. 84 WHAT ARE THE MOST COMMON OCCUPATIONAL FRAUD SCHEMES IN THE UNITED STATES AND CANADA?

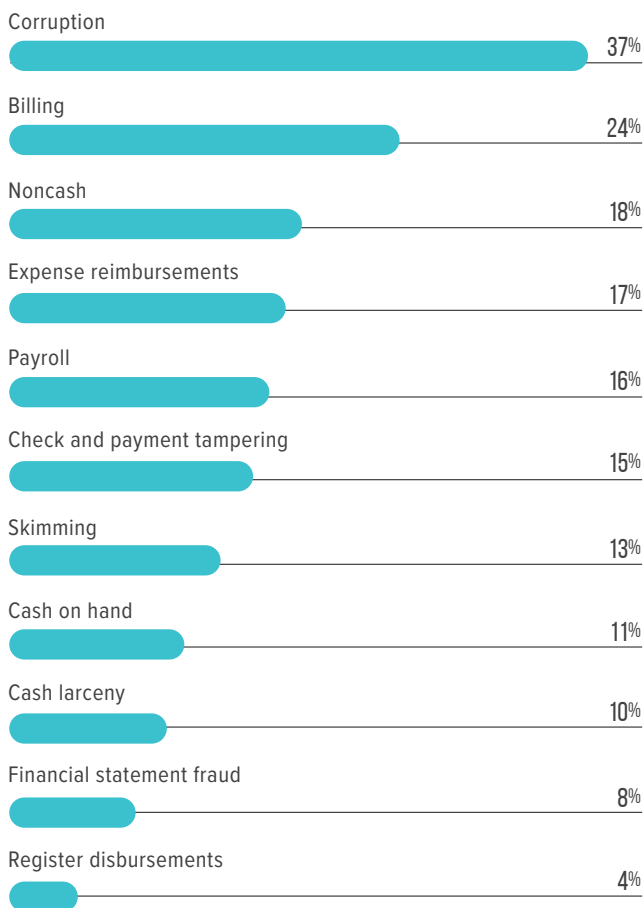


FIG. 85 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED IN THE UNITED STATES AND CANADA?



FIG. 86 WHAT ANTI-FRAUD CONTROLS ARE THE MOST COMMON IN THE UNITED STATES AND CANADA?

Control	Percent of cases
Code of conduct	74%
External audit of financial statements	72%
Employee support programs	66%
Internal audit department	66%
Management certification of financial statements	65%
External audit of internal controls over financial reporting	63%
Hotline	63%
Management review	63%
Independent audit committee	56%
Fraud training for employees	55%
Fraud training for managers/executives	55%
Anti-fraud policy	51%
Proactive data monitoring/analysis	43%
Formal fraud risk assessments	42%
Dedicated fraud department, function, or team	41%
Surprise audits	35%
Job rotation/mandatory vacation	20%
Rewards for whistleblowers	14%

FIG. 87 HOW DOES THE PERPETRATOR'S LEVEL OF AUTHORITY RELATE TO OCCUPATIONAL FRAUD IN THE UNITED STATES AND CANADA?

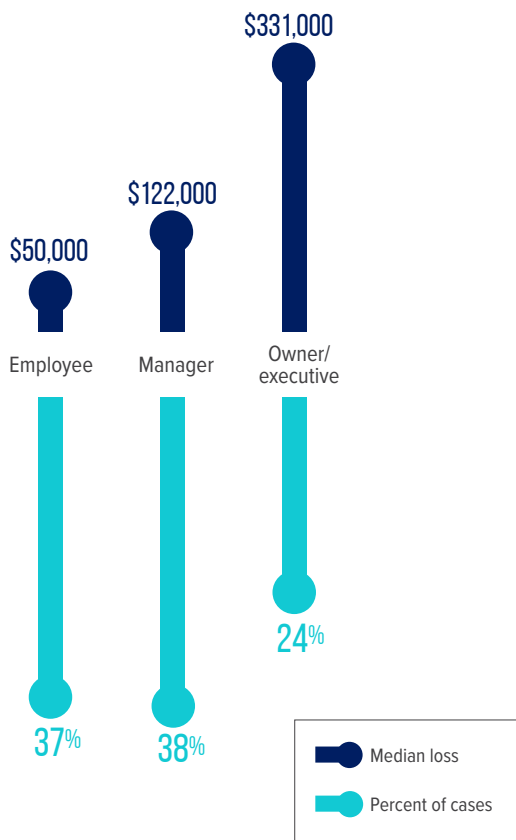
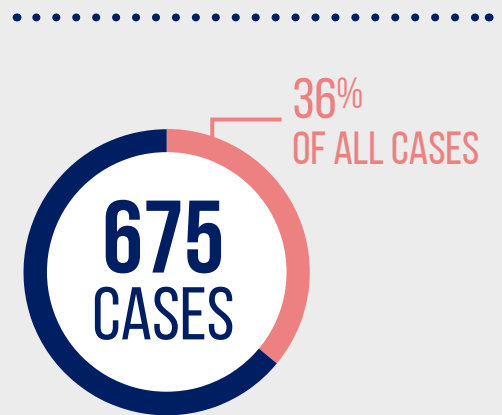


FIG. 88 CASES BY COUNTRY IN THE UNITED STATES AND CANADA

Country	Number of cases
Canada	50
United States	625
TOTAL CASES	675

MEDIAN LOSS:
USD 120,000



REGIONAL FOCUS

WESTERN EUROPE



FIG. 89 WHAT ARE THE MOST COMMON OCCUPATIONAL FRAUD SCHEMES IN WESTERN EUROPE?

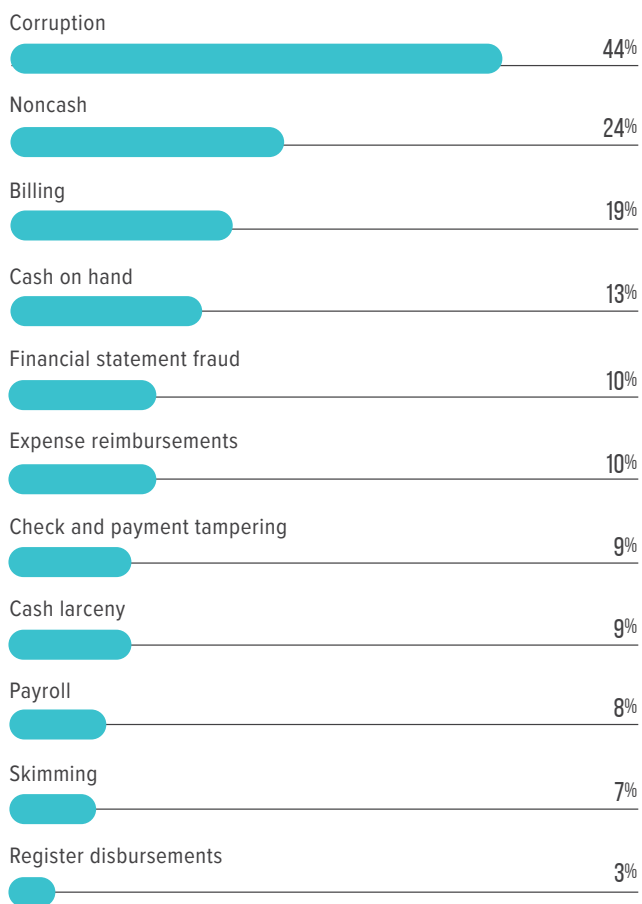


FIG. 90 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED IN WESTERN EUROPE?

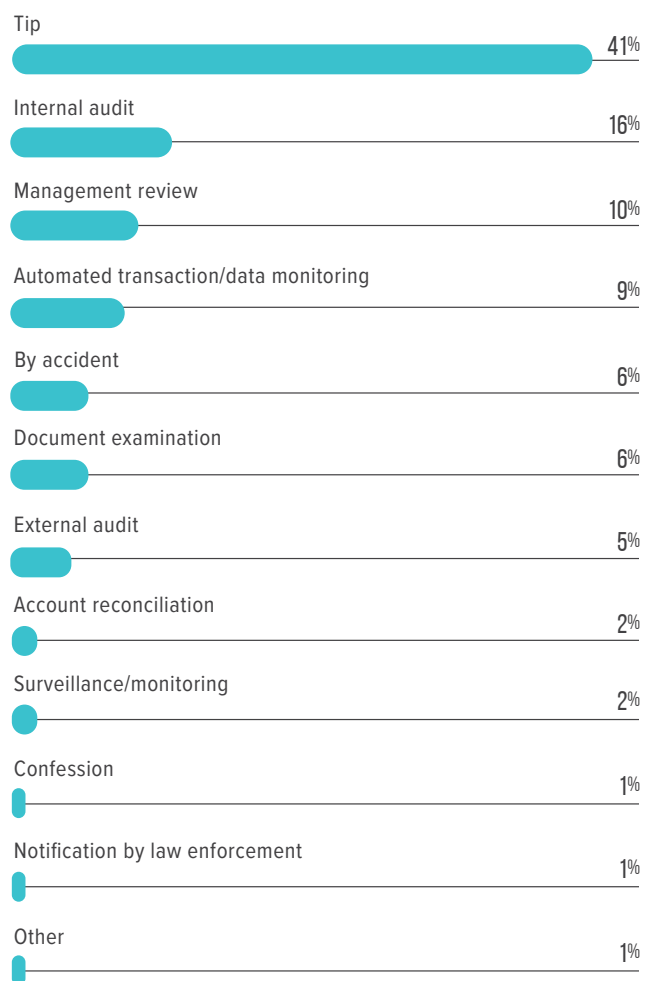


FIG. 91 WHAT ANTI-FRAUD CONTROLS ARE THE MOST COMMON IN WESTERN EUROPE?

Control	Percent of cases
External audit of financial statements	90%
Code of conduct	84%
Management certification of financial statements	78%
External audit of internal controls over financial reporting	77%
Internal audit department	74%
Management review	72%
Hotline	68%
Independent audit committee	65%
Fraud training for employees	59%
Fraud training for managers/executives	58%
Anti-fraud policy	56%
Formal fraud risk assessments	52%
Employee support programs	51%
Proactive data monitoring/analysis	48%
Dedicated fraud department, function, or team	47%
Surprise audits	40%
Job rotation/mandatory vacation	25%
Rewards for whistleblowers	7%

FIG. 92 HOW DOES THE PERPETRATOR'S LEVEL OF AUTHORITY RELATE TO OCCUPATIONAL FRAUD IN WESTERN EUROPE?

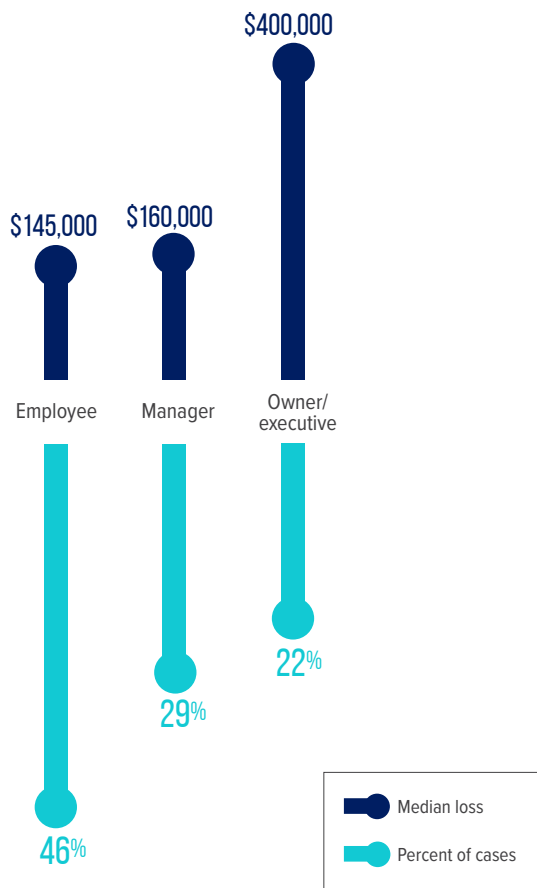
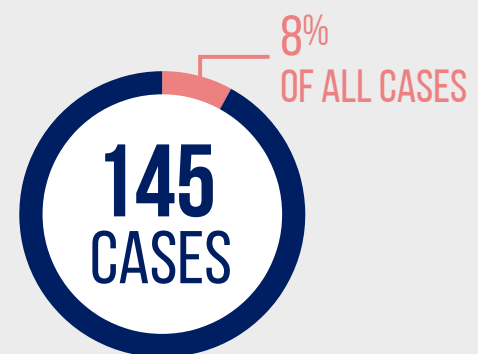


FIG. 93 CASES BY COUNTRY IN WESTERN EUROPE

Country	Number of cases
Aland Islands	1
Andorra	2
Austria	3
Belgium	5
Denmark	1
Finland	2
France	6
Germany	24
Greece	27
Ireland	3
Italy	17
Luxembourg	1
Netherlands	12
Norway	1
Spain	13
Switzerland	6
United Kingdom	21
TOTAL CASES	145

MEDIAN LOSS:
USD 173,000



STATISTICAL APPENDIX



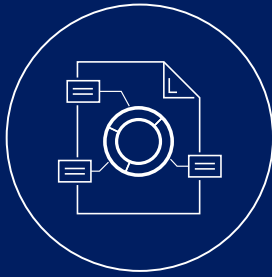
	Cases	25th percentile	Median (50th)	75th percentile	Mean*
ALL CASES†	2,046	\$20,000	\$117,000	\$600,000	\$1,783,000
Schemes					
Asset misappropriation	1,605	\$20,000	\$100,000	\$500,000	\$1,203,000
Noncash	284	\$10,000	\$78,000	\$500,000	\$921,000
Billing	281	\$20,000	\$100,000	\$500,000	\$852,000
Expense reimbursements	140	\$10,000	\$40,000	\$100,000	\$152,000
Skimming	137	\$10,000	\$50,000	\$188,000	\$185,000
Check and payment tampering	135	\$26,000	\$100,000	\$500,000	\$1,020,000
Cash on hand	129	\$5,000	\$15,000	\$100,000	\$131,000
Payroll	117	\$10,000	\$45,000	\$185,000	\$201,000
Cash larceny	103	\$10,000	\$45,000	\$389,000	\$6,920,000
Register disbursements	25	\$5,000	\$10,000	\$42,000	\$33,000
Corruption	906	\$25,000	\$150,000	\$1,000,000	\$2,647,000
Financial statement fraud	150	\$100,000	\$593,000	\$6,000,000	\$50,482,000
Detection method					
Tip	810	\$25,000	\$117,000	\$650,000	\$1,754,000
Internal audit	306	\$20,000	\$108,000	\$500,000	\$1,245,000
Management review	235	\$20,000	\$105,000	\$500,000	\$1,340,000
Document examination	107	\$37,000	\$200,000	\$1,500,000	\$2,256,000
By accident	105	\$25,000	\$100,000	\$730,000	\$1,293,000
Account reconciliation	91	\$10,000	\$74,000	\$370,000	\$985,000
Automated transaction/data monitoring	85	\$10,000	\$50,000	\$203,000	\$696,000
External audit	73	\$56,000	\$219,000	\$1,224,000	\$3,490,000
Surveillance/monitoring	51	\$5,000	\$60,000	\$350,000	\$1,127,000
Notification by law enforcement	34	\$148,000	\$500,000	\$6,150,000	\$5,185,000
Confession	16	\$29,000	\$159,000	\$8,375,000	\$5,521,000

*Mean amounts were calculated using loss data that was winsorized at 5% (i.e., assigned all cases in the top 2.5% and bottom 2.5% the same value as the 97.5th percentile and 2.5th percentile, respectively).

†Loss calculations were omitted for categories with fewer than ten responses.

	Cases	25th percentile	Median (50th)	75th percentile	Mean*
Victim organization					
Region:					
United States and Canada	663	\$20,000	\$120,000	\$649,000	\$1,460,000
Sub-Saharan Africa	425	\$15,000	\$100,000	\$352,000	\$1,841,000
Asia-Pacific	188	\$15,000	\$121,000	\$723,000	\$2,310,000
Western Europe	140	\$60,000	\$173,000	\$577,000	\$1,152,000
Middle East and North Africa	136	\$42,000	\$186,000	\$875,000	\$2,093,000
Southern Asia	130	\$10,000	\$92,000	\$500,000	\$1,490,000
Latin America and the Caribbean	94	\$33,000	\$175,000	\$915,000	\$1,550,000
Eastern Europe and Western/Central Asia	78	\$42,000	\$190,000	\$1,125,000	\$1,669,000
Organization type:					
Private company	851	\$20,000	\$120,000	\$550,000	\$1,389,000
Public company	484	\$25,000	\$118,000	\$735,000	\$1,694,000
Nonprofit	180	\$14,000	\$60,000	\$266,000	\$851,000
Government	346	\$20,000	\$138,000	\$800,000	\$2,522,000
National	157	\$40,000	\$200,000	\$1,450,000	\$3,319,000
State/provincial	91	\$15,000	\$56,000	\$503,000	\$2,306,000
Local	84	\$17,000	\$125,000	\$521,000	\$1,370,000
Organization size:					
<100 employees	423	\$25,000	\$150,000	\$550,000	\$1,373,000
100–999 employees	468	\$20,000	\$100,000	\$500,000	\$1,641,000
1,000–9,999 employees	543	\$16,000	\$100,000	\$500,000	\$1,704,000
10,000+ employees	476	\$24,000	\$138,000	\$900,000	\$1,973,000
Organization revenue:					
<\$50 million	720	\$20,000	\$100,000	\$400,000	\$1,027,000
\$50 million–\$499 million	496	\$20,000	\$105,000	\$644,000	\$1,821,000
\$500 million–\$999 million	222	\$27,000	\$150,000	\$1,150,000	\$2,840,000
\$1 billion+	455	\$25,000	\$150,000	\$973,000	\$2,076,000
Industry:					
Banking and financial services	341	\$15,000	\$100,000	\$368,000	\$1,739,000
Government and public administration	193	\$20,000	\$150,000	\$1,450,000	\$2,555,000
Manufacturing	191	\$35,000	\$177,000	\$1,000,000	\$1,755,000
Health care	126	\$18,000	\$100,000	\$600,000	\$1,392,000
Energy	95	\$30,000	\$100,000	\$1,000,000	\$1,793,000
Retail	89	\$15,000	\$65,000	\$375,000	\$1,024,000
Insurance	88	\$20,000	\$130,000	\$500,000	\$1,235,000
Technology	82	\$34,000	\$150,000	\$735,000	\$952,000
Transportation and warehousing	79	\$37,000	\$250,000	\$1,000,000	\$2,071,000
Construction	75	\$35,000	\$203,000	\$1,143,000	\$2,868,000
Education	67	\$10,000	\$56,000	\$306,000	\$1,022,000
Religious, charitable, or social services	58	\$20,000	\$78,000	\$275,000	\$323,000
Information (e.g., publishing, media, telecommunications)	58	\$20,000	\$58,000	\$500,000	\$714,000
Food service and hospitality	50	\$10,000	\$55,000	\$388,000	\$579,000
Services (professional)	41	\$33,000	\$125,000	\$625,000	\$1,716,000
Real estate	40	\$50,000	\$435,000	\$1,875,000	\$2,342,000
Arts, entertainment, and recreation	40	\$10,000	\$73,000	\$475,000	\$1,169,000
Agriculture, forestry, fishing, and hunting	39	\$15,000	\$154,000	\$1,500,000	\$2,114,000
Services (other)	31	\$15,000	\$100,000	\$268,000	\$417,000
Utilities	30	\$34,000	\$200,000	\$1,194,000	\$3,043,000
Wholesale trade	27	\$50,000	\$400,000	\$1,000,000	\$2,143,000
Mining	22	\$45,000	\$175,000	\$965,000	\$662,000

	Cases	25th percentile	Median (50th)	75th percentile	Mean*
Perpetrator					
Number of perpetrators:					
One perpetrator	773	\$12,000	\$57,000	\$269,000	\$896,000
Two perpetrators	360	\$29,000	\$145,000	\$750,000	\$1,499,000
Three or more perpetrators	691	\$42,000	\$219,000	\$1,300,000	\$2,638,000
Position:					
Employee	671	\$10,000	\$50,000	\$200,000	\$623,000
Manager	699	\$28,000	\$125,000	\$600,000	\$1,265,000
Owner/executive	411	\$80,000	\$337,000	\$2,380,000	\$3,928,000
Tenure:					
>10 years	359	\$50,000	\$250,000	\$1,200,000	\$2,357,000
6–10 years	448	\$27,000	\$137,000	\$500,000	\$1,568,000
1–5 years	839	\$15,000	\$100,000	\$450,000	\$1,439,000
<1 year	162	\$6,000	\$50,000	\$305,000	\$1,480,000
Department:					
Operations	269	\$14,000	\$74,000	\$500,000	\$1,133,000
Accounting	224	\$43,000	\$155,000	\$500,000	\$847,000
Executive/upper management	202	\$100,000	\$500,000	\$3,625,000	\$4,950,000
Sales	200	\$25,000	\$100,000	\$460,000	\$998,000
Customer service	136	\$10,000	\$40,000	\$248,000	\$765,000
Purchasing	130	\$33,000	\$129,000	\$700,000	\$1,672,000
Administrative support	129	\$19,000	\$90,000	\$298,000	\$421,000
Finance	93	\$31,000	\$160,000	\$1,000,000	\$1,324,000
Manufacturing and production	63	\$14,000	\$100,000	\$550,000	\$1,128,000
Warehousing/inventory	58	\$17,000	\$116,000	\$750,000	\$939,000
Board of directors	55	\$100,000	\$500,000	\$10,000,000	\$7,024,000
Information technology	53	\$25,000	\$150,000	\$625,000	\$2,240,000
Facilities and maintenance	44	\$6,000	\$58,000	\$475,000	\$1,143,000
Marketing/public relations	34	\$4,000	\$112,000	\$850,000	\$895,000
Human resources	27	\$38,000	\$100,000	\$165,000	\$136,000
Research and development	17	\$18,000	\$75,000	\$575,000	\$2,554,000
Gender					
Male	1,311	\$25,000	\$125,000	\$700,000	\$1,961,000
Female	480	\$15,000	\$100,000	\$382,000	\$753,000
Age					
<26	78	\$5,000	\$40,000	\$200,000	\$836,000
26-30	174	\$6,000	\$36,000	\$154,000	\$388,000
31-35	261	\$12,000	\$80,000	\$300,000	\$778,000
36-40	348	\$20,000	\$100,000	\$500,000	\$1,235,000
41-45	315	\$40,000	\$185,000	\$900,000	\$1,376,000
46-50	233	\$34,000	\$200,000	\$600,000	\$2,013,000
51-55	151	\$49,000	\$300,000	\$1,800,000	\$3,347,000
56-60	89	\$73,000	\$347,000	\$1,802,000	\$3,153,000
>60	47	\$125,000	\$800,000	\$7,978,000	\$6,487,000
Education level					
High school graduate or less	289	\$10,000	\$65,000	\$350,000	\$1,196,000
Some university	228	\$24,000	\$115,000	\$543,000	\$1,469,000
University degree	681	\$25,000	\$150,000	\$641,000	\$1,729,000
Postgraduate degree	251	\$33,000	\$135,000	\$1,000,000	\$2,613,000



INDEX OF FIGURES

Age of Perpetrator

How does the perpetrator's age relate to occupational fraud?	54
--	----

Anti-Fraud Controls

Spotlight: A Decade of Occupational Fraud: Trends from 2012–2022	18–19
Spotlight: COVID's Effect on Occupational Fraud	40
Did the background checks reveal existing red flags?	41
Spotlight: Hotline and Reporting Mechanism Effectiveness	24–25
How do anti-fraud controls vary by size of victim organization?	38
How does the perpetrator's age relate to occupational fraud?	54
How does the perpetrator's education level relate to occupational fraud?	55
How does the presence of anti-fraud controls relate to median loss?	36
How does the presence of anti-fraud controls relate to the duration of fraud?	37
Spotlight: Modifying Anti-Fraud Controls Following a Fraud	39
Top 3 internal control weaknesses based on the perpetrator's position	43
Was a background check run on the perpetrator prior to hiring?	41
What anti-fraud controls are most common?	34
What anti-fraud controls are the most common in various regions?	70–85
What are the primary internal control weaknesses that contribute to occupational fraud?	42
What types of background checks were run on the perpetrator prior to hiring?	41

Behavioral Red Flags of Perpetrator

Spotlight: Behavioral Red Flags of Fraud	60–61
Do fraud perpetrators experience negative HR-related issues prior to or during their frauds?	59
Spotlight: How Does Tenure Affect Fraud Risk?	48–49
How often do perpetrators exhibit behavioral red flags?	58

Which HR-related issues are most commonly experienced by fraud perpetrators?	59
--	----

Case Results

Spotlight: A Decade of Occupational Fraud: Trends from 2012–2022	18–19
Spotlight: How Does Tenure Affect Fraud Risk?	48–49
How do victim organizations punish fraud perpetrators?	62
Spotlight: Response to Fraud	63

Cost of Fraud

Spotlight: A Decade of Occupational Fraud: Trends from 2012–2022	18–19
Spotlight: Hotline and Reporting Mechanism Effectiveness	24–25
How does an organization's gross annual revenue relate to its occupational fraud risk?	30
How does an organization's size relate to its occupational fraud risk?	29
How does detection method relate to fraud loss and duration?	23
How do gender distribution and median loss vary based on the perpetrator's level of authority?	53
How does occupational fraud affect organizations in different industries?	32
Spotlight: How Does Tenure Affect Fraud Risk?	48–49
How does the duration of a fraud relate to median loss?	13
How does the number of perpetrators in a scheme relate to occupational fraud?	56
How does the perpetrator's gender relate to occupational fraud?	51
How does the perpetrator's level of authority relate to occupational fraud?	45
How does the perpetrator's tenure relate to occupational fraud?	46
How does the presence of anti-fraud controls relate to median loss?	36
How is occupational fraud committed?	9
Spotlight: Modifying Anti-Fraud Controls Following a Fraud	39

Spotlight: The Global Cost of Fraud	8
What departments pose the greatest risk for occupational fraud?	47
What is the typical velocity (median loss per month) of different occupational fraud schemes?	15
What levels of government are victimized by occupational fraud?	28
What types of organizations are victimized by occupational fraud?	28
Which asset misappropriation schemes present the greatest risk?	12

Concealment of Fraud Schemes

Spotlight: How Do Perpetrators Conceal Their Frauds?	17
--	----

Criminal and Employment Background of Perpetrator

Do perpetrators tend to have prior employment-related disciplinary actions for fraud?	57
Do perpetrators tend to have prior fraud convictions?	57

Demographics of Survey Participants

How many fraud cases have survey participants investigated in the past two years?	69
How much fraud examination experience did survey participants have?	69
What was the primary occupation of survey participants?	67
What was the professional role of the survey participants?	68

Department of Perpetrator

What are the most common occupational fraud schemes in high-risk departments?	50
What departments pose the greatest risk for occupational fraud?	47

Detection Method

Spotlight: Hotline and Reporting Mechanism Effectiveness	24–25
How does detection method relate to fraud loss and duration?	23
How is occupational fraud initially detected?	22
How is occupational fraud initially detected in various regions?	70–85
To whom did whistleblowers initially report?	27
What formal reporting mechanisms did whistleblowers use?	26
Who reports occupational fraud?	22

Duration of Fraud

Spotlight: COVID's Effect on Occupational Fraud	40
Spotlight: Hotline and Reporting Mechanism Effectiveness	24–25
How does detection method relate to fraud loss and duration?	23
Spotlight: How Does Tenure Affect Fraud Risk?	48–49
How does the duration of a fraud relate to median loss?	13

How does the perpetrator's level of authority relate to scheme duration?	45
How does the presence of anti-fraud controls relate to the duration of fraud?	37
How long do different occupational fraud schemes last?	14

Education Level of Perpetrator

How does the perpetrator's education level relate to occupational fraud?	55
--	----

Gender of Perpetrator

Spotlight: A Decade of Occupational Fraud: Trends from 2012–2022	18–19
Spotlight: Behavioral Red Flags of Fraud	60–61
How does the gender distribution of perpetrators vary by region?	52
How does the perpetrator's gender relate to occupational fraud?	51
How do gender distribution and median loss vary based on the perpetrator's level of authority?	53

Geographical Region of Victim Organization

Reported cases by region	7
Spotlight: Hotline and Reporting Mechanism Effectiveness	24–25
How does the gender distribution of perpetrators vary by region?	52
Asia-Pacific	70–71
Eastern Europe and Western/Central Asia	72–73
Latin America and the Caribbean	74–75
Middle East and North Africa	76–77
Southern Asia	78–79
Sub-Saharan Africa	80–81
United States and Canada	82–83
Western Europe	84–85

Industry of Victim Organization

How does occupational fraud affect organizations in different industries?	32
What are the most common occupational fraud schemes in various industries?	33

Number of Perpetrators

Spotlight: A Decade of Occupational Fraud: Trends from 2012–2022	18–19
Spotlight: How Does Tenure Affect Fraud Risk?	48–49
How does the number of perpetrators in a scheme relate to occupational fraud?	56

Position of Perpetrator

Spotlight: A Decade of Occupational Fraud: Trends from 2012–2022	18–19
Spotlight: Behavioral Red Flags of Fraud	60–61

Spotlight: How Does Tenure Affect Fraud Risk?	48–49
How does the perpetrator's level of authority relate to occupational fraud?	45
How does the perpetrator's level of authority relate to occupational fraud in various regions?	70–85
How does the perpetrator's level of authority relate to scheme duration?	45
How do gender distribution and median loss vary based on the perpetrator's level of authority?	53
Spotlight: Response to Fraud	63
Top 3 internal control weaknesses based on the perpetrator's position	43

Scheme Type

Spotlight: A Decade of Occupational Fraud: Trends from 2012–2022	18–19
Among frauds involving cryptocurrency, how was it used?	20
How do fraud schemes vary by organization size?	31
How is occupational fraud committed?	9
How long do different occupational fraud schemes last?	14
How often do fraudsters commit more than one type of occupational fraud?	11
Occupational Fraud and Abuse Classification System (The Fraud Tree)	10
What are the most common occupational fraud schemes in high-risk departments?	50
Spotlight: Response to Fraud	63

What are the most common occupational fraud schemes in various industries?	33
What are the most common occupational fraud schemes in various regions?	70–85
What is the typical velocity (median loss per month) of different occupational fraud schemes?	15
Which asset misappropriation schemes present the greatest risk?	12

Size of Victim Organization

Spotlight: Hotline and Reporting Mechanism Effectiveness	24–25
How does an organization's gross annual revenue relate to its occupational fraud risk?	30
How does an organization's size relate to its occupational fraud risk?	29
How do anti-fraud controls vary by size of victim organization?	38
How do fraud schemes vary by organization size?	31

Tenure of Perpetrator

Spotlight: How Does Tenure Affect Fraud Risk?	48–49
How does the perpetrator's tenure relate to occupational fraud?	46

Type of Victim Organization

Spotlight: Modifying Anti-Fraud Controls Following a Fraud	39
What levels of government are victimized by occupational fraud?	28
What types of organizations are victimized by occupational fraud?	28

FRAUD PREVENTION CHECKLIST



The most cost-effective way to limit fraud losses is to prevent fraud from occurring in the first place. This checklist is designed to help organizations test the effectiveness of their fraud prevention measures. Additional guidance, resources, and tools for managing organizational fraud risk can be found at [ACFE.com/fraudrisktools](https://www.acfe.com/fraudrisktools).

1. Is ongoing anti-fraud training provided to all employees of the organization?

- Do employees understand what constitutes fraud?
- Have the costs of fraud to the company and everyone in it—including lost profits, adverse publicity, potential job loss, and decreased morale and productivity—been made clear to all employees?
- Do employees know where to seek advice when faced with uncertain ethical decisions, and do they believe that they can speak freely?
- Has a policy of zero-tolerance for fraud been communicated to employees through words and actions?

2. Is an effective fraud reporting mechanism in place?

- Have employees been taught how to communicate concerns about known or potential wrongdoing?
- Are one or more reporting channels (e.g., a third-party hotline, dedicated email inbox, or web-based form) available to employees?
- Do employees trust that they can report suspicious activity anonymously and/or confidentially (where legally permissible) and without fear of reprisal?
- Has it been made clear to employees that reports of suspicious activity will be promptly and thoroughly evaluated?
- Do reporting policies and mechanisms extend to vendors, customers, and other outside parties?
- Do reporting mechanisms include multilingual capabilities and provide access to a trained interviewer 24 hours a day, 7 days a week?

3. To increase employees' perception of detection, are the following proactive measures taken and publicized to employees?

- Is possible fraudulent conduct aggressively sought out, rather than dealt with passively?
- Are surprise fraud audits performed in addition to regularly scheduled audits?
- Are data analytics techniques used to proactively search for fraud and, if so, has the use of such techniques been made known throughout the organization?
- Do managers actively review the controls, processes, accounts, or transactions under their purview for adherence to company policies and expectations?

4. Is the management climate/tone at the top one of honesty and integrity?

- Are employees periodically surveyed to determine the extent to which they believe management acts with honesty and integrity?
- Are performance goals realistic and clearly communicated?
- Have fraud prevention goals been incorporated into the performance measures that are used to evaluate managers and to determine performance-related compensation?
- Has the organization established, implemented, and tested a process for oversight of fraud risks by the board of directors or others charged with governance (e.g., the audit committee)?

5. **Are fraud risk assessments performed to proactively identify and mitigate the company's vulnerabilities to internal and external fraud?**
 - Are fraud risk assessments updated regularly (e.g., annually), as well as following times of notable organizational or environmental changes?
 - Are the results of the fraud risk assessment shared with appropriate levels of management and used to update the organization's anti-fraud program and controls?

6. **Are strong anti-fraud controls in place and operating effectively, including the following?**
 - Proper separation of duties
 - Use of authorizations
 - Physical safeguards
 - Job rotations
 - Mandatory vacations

7. **Does the internal audit department, if one exists, have adequate resources and authority to operate effectively and without undue influence from senior management?**

8. **Does the hiring policy include the following (where permitted by law)?**
 - Past employment verification
 - Criminal and civil background checks
 - Credit checks
 - Drug screening
 - Education verification
 - References checks

9. **Are employee support programs in place to assist employees struggling with addiction, mental/emotional health, family, or financial problems?**

10. **Is an open-door policy in place that allows employees to speak freely about pressures, providing management the opportunity to alleviate such pressures before they become acute?**

11. **Are regular, anonymous surveys conducted to assess employee morale?**

GLOSSARY OF TERMINOLOGY



Asset misappropriation: A scheme in which an employee steals or misuses the employing organization's resources (e.g., theft of company cash, false billing schemes, or inflated expense reports)

Billing scheme: A fraudulent disbursement scheme in which a person causes their employer to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases (e.g., employee creates a shell company and bills employer for services not actually rendered; employee purchases personal items and submits an invoice to employer for payment)

Cash larceny: A scheme in which an incoming payment is stolen from an organization after it has been recorded on the organization's books and records (e.g., employee steals cash and checks from daily receipts before they can be deposited in the bank)

Cash-on-hand misappropriations: A scheme in which the perpetrator misappropriates cash kept on hand at the victim organization's premises (e.g., employee steals cash from a company vault)

Check or payment tampering scheme: A fraudulent disbursement scheme in which a person steals their employer's funds by intercepting, forging, or altering a check or electronic payment drawn on one of the organization's bank accounts (e.g., employee steals blank company checks and makes them out to themselves or an accomplice; employee re-routes an outgoing electronic payment to a vendor to be deposited into their own bank account)

Corruption: A scheme in which an employee misuses their influence in a business transaction in a way that violates their duty to the employer in order to gain a direct or indirect benefit (e.g., schemes involving bribery or conflicts of interest)

Employee support programs: Programs that provide assistance to employees dealing with personal issues or challenges, such as counseling services for addiction, family, or financial problems

Expense reimbursements scheme: A fraudulent disbursement scheme in which an employee makes a claim for reimbursement of fictitious or inflated business expenses (e.g., employee files fraudulent expense report claiming personal travel or nonexistent meals)

Financial statement fraud: A scheme in which an employee intentionally causes a misstatement or omission

of material information in the organization's financial reports (e.g., employee files fraudulent expense report claiming personal travel or nonexistent meals)

Fraudulent disbursement scheme: A scheme in which an employee makes a distribution of organizational funds or manipulates a disbursement/payment function for a dishonest purpose (e.g., submitting false invoices for payment, altering time cards, or making personal purchases with company funds)

Hotline: A mechanism to report fraud or other violations, whether managed internally or by an external party. This might include telephone hotlines, dedicated email addresses, web-based platforms, and other mechanisms established to facilitate fraud reporting.

Management review: The process of management reviewing organizational controls, processes, accounts, or transactions for adherence to company policies and expectations

Noncash misappropriations: A scheme in which an employee steals or misuses noncash assets of the victim organization (e.g., employee steals inventory from a warehouse or storeroom; employee steals or misuses confidential customer information)

Occupational fraud: The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets

Payroll scheme: A fraudulent disbursement scheme in which an employee causes their employer to issue a payment by making false claims for compensation (e.g., employee claims overtime for hours not worked; employee adds ghost employees to the payroll)

Primary perpetrator: The person who worked for the victim organization and who was reasonably confirmed as the primary culprit in the case

Register disbursements scheme: A fraudulent disbursement scheme in which an employee makes false entries on a cash register to conceal the fraudulent removal of cash (e.g., employee fraudulently voids a sale on a cash register and steals the cash)

Skimming: A scheme in which an incoming payment is stolen from an organization before it is recorded on the organization's books and records (e.g., employee accepts payment from a customer but does not record the sale and instead pockets the money)

ABOUT THE ACFE



Founded in 1988 by Dr. Joseph T. Wells, CFE, CPA, the Association of Certified Fraud Examiners (ACFE) is the world's largest anti-fraud organization and premier provider of anti-fraud training and education. Together with more than 90,000 members, the ACFE is reducing business fraud worldwide and inspiring public confidence in the integrity and objectivity within the profession.

The ACFE unites and supports the global anti-fraud community by providing educational tools and practical solutions for professionals through events, publications, networking, and educational materials for colleges and universities.

CERTIFIED FRAUD EXAMINERS

The ACFE offers its members the opportunity for professional certification with the Certified Fraud Examiner (CFE) credential. The CFE is preferred by businesses and government entities around the world, and indicates expertise in fraud prevention and detection. CFEs are anti-fraud experts who have demonstrated knowledge in four critical areas: Financial Transactions and Fraud Schemes, Law, Investigation, and Fraud Prevention and Deterrence.

MEMBERSHIP

Members of the ACFE include accountants, internal auditors, fraud investigators, law enforcement officers, lawyers, business leaders, risk/compliance professionals, and educators, all of whom have access to expert training, educational tools, and resources. Whether their career is focused exclusively on preventing and detecting fraudulent activities or they just want to learn more about fraud, the ACFE provides anti-fraud professionals with the essential tools and resources necessary to accomplish their objectives.

To learn more, visit [ACFE.com](https://www.acfe.com) or call (800) 245-3321 / +1 (512) 478-9000.

CONTACT

Association of Certified Fraud Examiners
Global Headquarters
716 West Ave | Austin, TX 78701-2727 | USA
Phone: (800) 245-3321 / +1 (512) 478-9000
[ACFE.com](https://www.acfe.com) | info@acfe.com

TERMS OF USE

Occupational Fraud 2022: A Report to the Nations is available for use free of charge as a public service of the ACFE. You may download, copy and/or distribute the report for personal or business use on the following conditions:

1. No portion of *Occupational Fraud 2022: A Report to the Nations* may be sold or otherwise licensed, shared or transferred to any party for a fee, or included in any work that is to be sold, licensed, shared or transferred to any party for a fee, without the express written consent of the ACFE. The foregoing notwithstanding, you are permitted to use the report as part of a speech or presentation for which an admission fee is charged.
2. *Occupational Fraud 2022: A Report to the Nations* must be properly attributed to the ACFE, including the name of the publication. An example of proper attribution is: "*Occupational Fraud 2022: A Report to the Nations*. Copyright 2022 by the Association of Certified Fraud Examiners, Inc."



[ACFE.com/RTTN](https://www.acfe.com/RTTN)

© 2022 Association of Certified Fraud Examiners, Inc.
“ACFE,” “CFE,” “Certified Fraud Examiner,” “CFE Exam
Prep Course,” “Fraud Magazine,” “Association of Certified
Fraud Examiners,” “Report to the Nations,” the ACFE seal,
the ACFE logo and related trademarks, names and logos
are the property of the Association of Certified Fraud
Examiners, Inc., and are registered and/or used in the U.S.
and countries around the world.