OCCUPATIONAL FRAUD:

A Hidden Killer of Organizational Performance

A Guide to Understanding, Detecting, and Recovering from Occupational Fraud to Protect the Health of Your Company

LowersRiskGroup®

EXECUTIVE SUMMARY:

What Constitutes Occupational Fraud and Why Should You Be Concerned?

Occupational fraud is a largely hidden threat to the bottom line of almost every organization in our economy worldwide. Also known as employee theft or embezzlement, occupational fraud describes a range of willful employee misconduct through which businesses lose money.

No industry is exempt, with a collective global cost estimated at more than

$3.7 TRILLION ANNUALLY.[1,6]

While fraud is often not even detected and is commonly a concealed destroyer, it's one worth shining a bright light on and taking strong measures to detect and address. It pays to pay attention here.

For, with controls, it can be prevented or at least mitigated. While only an estimated 14% of defrauded organizations recover their losses in full, more than **50% of businesses with controls in place are able to detect, mitigate, or resolve fraud incidents to some degree.**[5,6] Even if the outcome of one incident is disciplinary action taken to use as an example to others, or is tightening controls to prevent future loss, this can be a manageable jolt compared to the havoc that can happen without any controls in place.

Victim organizations typically lose about 5% of revenues per year, with a median loss of $150,000 per incident. Larger losses can represent more than a million dollars per incident, or even multi-million dollar losses for a single incident. For a problem cloaked and concealed, the cost is anything but invisible – it's devastating and can result in the crippling of businesses large and small.[1]

Most frauds go undetected entirely or are uncovered either by accident or as the result of a whistleblower.[1] If there is good news about this topic, it is this: an organization can transform risk into an effective fraud prevention program in 3 steps - all thoroughly covered in this guide:

- ✓ **Understand what fraud is and how it is likely to emerge or present itself.**
- ✓ **Identify potential sources of fraud in your organization.**
- ✓ **Take steps to prevent and/or resolve fraud through processes or controls.**

In this guide you will learn both the scope of the problem and what you can do about it. You'll learn about the importance of cultivating a top-down, anti-fraud corporate culture that permeates throughout all departments. And while this can take time to build and requires continuous effort to sustain, in the end it is a worthwhile investment to protect the whole of your business, including your people, your profits, and your brand.

EMPLOYEE MISCONDUCT FOR PERSONAL GAIN:

Understanding Occupational Fraud Schemes

Occupational fraud is a ubiquitous problem – searing a costly graze across the globe, impairing companies of any size and nearly every industry. It is most simply defined as the willful misconduct of an employee that results in a business losing money. In other words, anytime someone deliberately misuses or misapplies the resources or assets of a business for their own personal benefit. And it stings, $3.7 trillion worth of sting every year.[1,6]

UNFORTUNATELY, OCCUPATIONAL FRAUD IS A GROWING INDUSTRY.

Estimated global losses of $3.5 trillion grew to $3.7 trillion - over just two short years.[6,7,8]

Occupational fraud takes many forms, from petty theft to sophisticated swindles that cost millions, and can be classified into 3 categories:

Asset Misappropriations: Fraudsters steal or misuse an organization's assets (can include cash and non-cash schemes).

Corruption: Perpetrators use their organizational authority or influence to obtain an unauthorized personal material benefit from a business transaction involving their employer.

Financial Statement Fraud: The perpetrator falsifies the organization's financial statements to divert assets, making it appear more or less profitable for personal gain.[1]

In addition to being categorized, a fraud scheme is generally defined by these four common elements:

1 | It is clandestine (proactively concealed and not easily detected);

2 | It involves a violation of the perpetrator's fiduciary responsibility to the employer;

3 | It is intended to materially benefit the perpetrator;

4 | And it imposes costs on the employer. [5]

In the end, occupational fraud is a crime that violates the basic trust an employer or organization puts in a person. In many cases, especially those involving financial statement fraud, the perpetrator is often a person with considerable authority and/or is a highly trusted leader within the company, or a close friend or family member. No department or position is exempt, a top-to-bottom zero tolerance policy, a code of conduct, and other controls are critical for every organization. Later in this guide we offer information about perpetrator profiles and red flag behaviors.

Below is a closer look at the fraud schemes found within the 3 main categories: asset misappropriation, corruption, and financial report misstatement. Understanding the problem is the first step to understanding how to protect your organization's productivity and profits.[1,2]

ASSET MISAPPROPRIATION

83.5% OF CASES

MEDIAN LOSS:
$125K

Theft of Cash-on-hand
Theft of Cash Receipts
Fraudulent Disbursements
Non-cash Theft (Inventory)

CORRUPTION

35.4% OF CASES

MEDIAN LOSS:
$150K

Conflict of Interest
Bribery
Illegal Gratuities
Economic Extortion

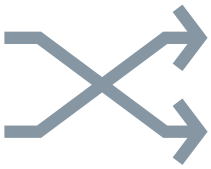
FINANCIAL STATEMENT

9.6% OF CASES

MEDIAN LOSS:
$975K

Asset Understatement
Asset Overstatement

FRAUD SCHEMES[1,4,5]



ASSET MISAPPROPRIATION: STEALING OR MISUSING RESOURCES

Definition: *Any scheme in which an employee steals or misuses the employing organization's resources.*

As the most common of the three types of fraud, asset misappropriation occurs in more than 80% of reported cases, costing a median $125,000 per incident. This category includes the direct stealing of cash, indirectly stealing through cash receipt scams, accounts receivable scams, fraudulent disbursements, and inventory schemes.

Indirect stealing can take many forms:

SKIMMING

Skimming happens in various ways and is defined as stealing prior to the revenues even hitting the company's books. This can be intercepted checks, unreported sales, or misstated sales where the unreported balance is pocketed by the fraudster.

CASH LARCENY

Cash larceny, which is "on-book" theft where the fraudster intentionally takes an employer's cash (including currency and/or receipts/checks) without the consent and violating the agreements of the employing company.

FRAUDULENT DISBURSEMENTS

Fraudulent disbursements are the most common form of asset misappropriation, occurring when an employee uses his position of employment to result in a payment for some inappropriate purpose. These disbursements are on-book, meaning that cash (or checks) are distributed fraudulently, but gets recorded thus leaving an audit trail. Fraudulent disbursement schemes include the following types:

- **Check tampering schemes** – either preparing a fraudulent check for personal gain or intercepting a check intended for payment to a third party. This is the most direct form of fraud as the perpetrator physically interferes with a cash instrument: forging a signature, altering a payee or the amount of a check, and/or forging an endorsement.

- **Register disbursement schemes** – including refunds and voided sales, these are classified as fraudulent disbursements. Because an employee physically removes cash from the cash register and absconds with it, such schemes are similar to cash larceny schemes.

- **Billing schemes** – cause the victim organization to buy goods or services that are nonexistent, overpriced, or not needed by the organization. The fraudulent support documents, which can include invoices, purchase orders, purchase requisitions, receiving reports, etc., cause the victim organization to issue a check which then gets cashed or redirected by the perpetrator toward an illegal benefit.

- **Expense reimbursement schemes** – employees falsify information about their business expenses and cause their employers to overcompensate them.

- **Payroll schemes** – similar to billing schemes, where a perpetrator produces some false document or otherwise makes a false claim for a distribution of funds by his employer. In payroll schemes, the fraudster falsifies payroll records, timekeeping records, or some other document concerned with the payroll function.

NON-CASH MISAPPROPRIATIONS

The final type of scheme in this category is non-cash misappropriations such as accounts receivable, inventory or fixed asset schemes. This category can include lapping (overlapping payments), fictitious receivables, misposting account credits, converting inventory for personal use or outright stealing it, illegal gratuities, bid rigging or market division fraud (the latter two generally require collusion between multiple parties and cross over into the next category, corruption).

Some simple controls in place such as two signatures or a verification process can halt and control many misappropriation incidents. As the most common category, these controls can truly "pay off", both figuratively and literally.

CORRUPTION:
VIOLATING DUTY FOR PERSONAL GAIN

Definition: *A scheme in which an employee misuses his or her influence in a business transaction in a way that violates his or her duty to the employer in order to gain a direct or indirect benefit.*

Corruption is the use of influence in a business deal to procure a benefit for the perpetrator or another colluding person, an outcome contrary to the duty and/or the rights of the employer or others involved. Corruption occurs in various forms, including conflicts of interest (sales or purchasing schemes), bribery, kickbacks, illegal gratuities, and economic extortion.

The recipients of these schemes can range from a low-level clerk to a chief executive officer or even a public official - there is no level of an organization that is exempt. Sometimes schemes involve multiple levels of employees or multiple departments working together within an organization (colluding) which is also considered corruption.

FINANCIAL STATEMENT FRAUD:
INTENTIONAL REPORT ALTERATION FOR PERSONAL GAIN

Definition: *A scheme in which an employee intentionally misrepresents or omits of material information in the organization's financial reports, resulting in a personal gain. Financial reporting fraud or financial statement fraud assumes the misrepresentation results from an intentional failure to follow accepted accounting principles, a serious concern for investors or other stakeholders.*

Schemes can include:

- Timing Differences
- Fictitious Revenues
- Concealed Liabilities & Expenses
- Improper Asset Valuation
- Improper Disclosures
- Timing Differences
  - Understated Revenues
  - Overstated Liabilities & Expenses
  - Improper Asset Valuation

THE DEVASTATING GLOBAL IMPACT OF OCCUPATIONAL FRAUD

Though the schemes may be hidden, the effects of occupational fraud are obvious and go directly to the bottom line. Fraud can deteriorate all strata of a business between the perpetrator and the bottom line. Fraud raids profits and deprives employees, businesses, government agencies, non-profits, potentially ANY organization of the growth and success it deserves and is actually producing.

This shrouded nemesis hurts organizations at multiple levels of performance and is costly in more ways than revenues alone. Reputation, productivity, morale and security are often also damaged. There is also another devastating hit - multiple cases of financial reporting fraud have undermined the basic confidence in the U.S. capital markets,

A COMPLETELY SILENT KILLER OF INVESTMENT PRODUCTIVITY

for many public companies across the global market.[1]

20% of reported cases result in

OVER $1 MILLION OF LOSS

THE BOTTOM LINE ON LOSS

The Association of Certified Fraud Examiners (ACFE) reports that organizations dealing with occupational fraud typically lose around 5% of revenue each year. In dollars, that equates to projected annual losses in excess of $3.7 trillion worldwide. The 2016 ACFE Report to the Nations published the median occupation fraud loss at approximately $140,000-$150,000, with more than 20% of reported cases resulting in over $1 million of loss. These are devastating losses that can be crippling, even cause an organization to file bankruptcy or fail, imploring a clear step toward instituting, consistently utilizing and evaluating an entity's internal controls and risk assessment plans. Controls can make THE difference in prevention, detection, and recovery.[1,2]

OCCUPATIONAL FRAUD BY REGION

While the leading category may vary region to region, it is evident that this 'hidden' killer can be found anywhere and everywhere in the world. The graphic below shows the median scheme loss per region. [1,2]

While HIDDEN is a term often used when referring to the problem of occupational fraud, certain key factors are conspicuous and earmark the potential degree of impact. These factors also point to the particular solutions that can prevent or minimize the damage. Below are a few of the highest offending factors that, when known, can be monitored with quality controls to mitigate loss.

Scheme[1,2]

Each scheme category causes a unique impact.

- Misappropriations are the most common scheme, infiltrating its impact across all layers of organizations from C-suites to mailrooms. Even though the median losses are considerably less than the other categories, at 80%+ of the volume of cases, this category overall has the widest impact on performance. Because it is common, it makes sense for all organizations to have controls to detect and proactively halt this type of scheme.

  Asset Misappropriation: $125K median global loss

- The impact of corruption schemes can be the most diverse as the primary weapon is authority and influence. Corruption undermines basic human resources infrastructure of an organization by deteriorating trust internally and often externally or both. Corruption is often referred to as a relationship killer because it silently jeopardizes the organization's ability to nurture trust in its brand.

  Corruption: $200K median global loss

- By far, financial statement fraud generates the greatest median loss per scheme. The dollars themselves are grievous and severe. The trust factor, here, however, can be the most shocking and devastating factor as the perpetrators can be the most highly trusted leaders or authorities within an organization. Recovering from damage of this kind of betrayal is often impossible. This type of fraud has even undermined the general culture of capital market trading.

  Financial Statement Fraud: $975K median global loss

Defense:

No matter which category of scheme at hand, these top three defense maneuvers can begin to shift the weakness toward prevention.

- Top to bottom corporate control systems/ policies with C-level endorsement and engagement
- Zero tolerance for breach of policy
- Anonymous systems for reporting

Authority[1,3]

Who the perpetrator is (or who they are if there is collusion) makes a big difference on the impact of a scheme on an organization. The greater the authority, the greater the loss. And the higher up the ladder a scheme travels, the other risk factors also inflate - reputation, productivity, security, and morale. On average, owner or executive perpetrators cause median damage more than 10X employee perpetrator schemes.

Owner exec: $703K median loss
Manager: $173K median loss
Employee: $65K median loss

Defense:

- Multi-level, cross departmental reporting structures and checks & balances
- Internal and external reviewers
- Code of conduct reviewed and affirmed organization wide on a regular basis

Collusion

Once multiple parties get involved in a scheme together, the losses begin to rise. Without exception, the more people involved, the higher the losses.[2]

1 person: $85K median loss
2 people: $150K median loss
3 people: $220K median loss
4 people: $294K median loss
5+ people: $633K median loss

Defense:

- Multi-level, cross departmental reporting structures and checks & balances
- Code of conduct reviewed and affirmed organization wide on a regular basis
- Anonymous systems for reporting

Duration[2]

Because fraud is intentionally concealed by the perpetrators, it often is difficult to detect for some time. The longer the scheme goes on, the greater the fiscal damage WILL be.

- The median duration worldwide across all scheme categories is 18 months, resulting in a median loss of $150,000 per incident.
- When a scheme goes on for more than 5 years, the median losses are exponentially more destructive at $850K per incident.

Defense:

- Frequent reporting and review cycles
- Internal and external reviewers

LEGAL END GAME

Another aspect of organizational impact is the end result of each incident. Many organizations don't end up pursuing legal action because the publicity of an event could cause far more damage than the fiscal sting of the incident itself. When cases do go forward, however, suits are won by the victim organization nearly 80% of the time.[1]

VICTIM ORGANIZATIONS: WHO IS (MORE) SUSCEPTIBLE AND WHY[1,5]

To expose, prevent, and mitigate the hidden killer that occupational fraud can be requires understanding more than just what fraud is. The "who" factor (both victim and perpetrator) is also a pathway to stopping loss before it happens or before it reaches an irrecoverable point of destruction.

Recorded victims of occupational fraud are diverse. Victims include private and public companies, not-for-profits, governmental agencies, and any other kind of organization where managers and employees have access to financial or material assets. While fraud may be somewhat more likely among certain types of organizations (e.g., for-profit suffer more than non-profit, and banking/financial services organizations experience the highest number of cases) or occupations (e.g., accounting or sales), it is truly an equal opportunity threat in the sense that it can occur anywhere and anytime factors combine to create the opportunity.

Here is a breakdown of key organizational factors consistent within many victim organizations:
In addition to being categorized, a fraud scheme is generally defined by these four common elements:

LEADERSHIP FOCUS IS DIVERTED

Busy owners can become deceived owners. When organizational leadership is focused too much on operations, productivity and the bottom line, red flags can be missed or the systematic reviews required to detect fraud can be altogether absent, seeming to be an administrative headache or a waste of time. Sometimes slowing down is the antidote to be able to keep an organization moving toward its goals the fastest.

If not anticipated, by the time a case is discovered, it's often too late to recover.

- **Where controls do exist, 20% of reported cases revealed an override of existing internal controls. Active management and oversight of the controls is imperative for them to be effective.**
- **The smaller the organization, understandably, the easier it is to neglect or overlook the implementation of anti-fraud controls. However, this gap in prevention and detection procedures leaves smaller organizations susceptible to fraud that can cause destruction to the limited resources available.**
- **Often business owners or executives are shocked by WHOM the perpetrator ends up being. If they are too busy to really pay attention to what is happening for the perpetrator, if they are not highly attuned to the potential red flags, they can be stunned at a scheme run by a long term, trusted employee, a fellow executive or board member, a partner or even a close friend.**

SMALLER ORGANIZATIONS CAN BE MORE AT RISK

When it comes to the risk of occupational fraud, size (of an organization) does matter. For small businesses it can be a financial risk to 'bother' with putting controls in place and extending resources to try to manage those controls. But without it, smaller businesses can be instantly debilitated, forced into bankruptcy and essentially ruined or forced to close by one incident. The protective measures ensure performance rather than threaten success.

- **For-profits suffer slightly larger median losses and many more reported cases:**
  - Privately held $180K median loss
  - Publicly owned $178K median loss
- **Of government cases, federal fraud is the most costly:**
  - Federal $194K median loss
  - State or provincial $100K
  - Local $80K
- **Median loss is the same whether the company is big or small, but its impact is much greater, even debilitating for the smaller organization.**
- **Different size organizations have different fraud risks.**
  - Smaller entities are generally more at risk than larger ones
  - Corruption is prevalent in larger organizations

CERTAIN INDUSTRIES AND DEPARTMENTS ARE MORE AT RISK

If your company falls under one of these industries, or works closely with one, the risk of occupational fraud is highest and measures should be taken immediately if they are not already in place:

- **Banking**
- **Financial Services**
- **Government**
- **Public Administration**
- **Manufacturing**
- **Mining and wholesale trading have fewest cases but greatest median losses $500K and $450K**
- **Department**
  - Accounting office/department (16.6%) than any other biz unit
  - Three-quarters of fraud comes from one of seven key departments:
    - Accounting
    - Operations
    - Sales
    - Exec/upper management
    - Customer service
    - Purchasing
    - Finance

There are also some typical organizational behaviors that are known to be red flags for victims. The cumulative effect of these red flag behaviors is opportunity. Avoid these behaviors and protect your performance and profits.

- Using suspicious or unfamiliar financial partners, from banks to accountants
- Incomplete, missing, or non-standard documentation used in business dealings
- Suspicious or unfamiliar subsidiary companies or entities (could be established to conceal illegal activities)
- Sloppy, secretive, or irregular accounting records
- Non-adherence to company policies, including subordinates being directed to bend or break rules
- Exclusive or preferred treatment of vendors, often under the guise of sole source contracts
- Existence of evergreen contracts (no end date or review)
- Previous complaints, allegations, or concerns over company or employee conduct
- Conflicts of interest are common rather than an exception
- Organizational absence or confusion about ethics or core values
- Key individual and/or organizational due diligence comes back missing or negative
- 25% or more of business with a single customer
- Performance-based remuneration (i.e. results-at-all-costs attitude)

PERPETRATOR PROFILE[1,4,5,8]

Every organization is at risk of fraud and every organization can lower that risk with the right approach. Recognition is the first step to prevention. Most crimes of occupational fraud are motivated, at least in part, by some kind of financial pressure. And while committing a fraud, the perpetrator will frequently display certain predictable behavioral traits associated with the stress or fear of being caught.

A proven tool known as the **Fraud Triangle** encapsulates the most common behavior scenario of most fraudsters. Perpetrators usually have at least one of these if not all three:

1 | **Perceived financial need**

2 | **Perceived opportunity**

3 | **The ability to rationalize or justify the illegal conduct**

IN MORE THAN 80% OF CASES, A PERPETRATOR DISPLAYS AT LEAST ONE

(usually more than one) of these behavioral red flags.

The "red flags" are clues that can be picked up by attentive managers, colleagues, internal auditors, or subordinates. In turn, these clues can put an organization "on notice" that a trusted individual may be involved in some form of improper conduct and effective measures can commence, protecting performance and preventing disasters.

Here are the other typical red flags:

4 | **Authority Impact**

Perpetrator level of authority correlates directly with the fiscal impact of a fraud scheme. Therefore it is essential to put more and tighter controls in place the closer you get to the C-suite.

- **Owners/Execs**–$703K median loss/incident
  - 4x higher than managers @ $173K
  - 11x higher than employees @ $65K
- **Managers**–$173K median loss/incident
- **Employees**–$65K median loss/incident

5 | **Perpetrator Behavior Warning Signs**

- Living beyond means
- Financial difficulties
- Unusually close associations with vendors or customers
- Excessive control issues
- General wheeler-dealer attitude involving unscrupulous behavior
- Recent divorce or family problems

With some proactive tools and a commitment to attentiveness, businesses can identify employees with a propensity for this misbehavior and protect departmental and company performance.

OCCUPATIONAL FRAUD SOLUTIONS: WHAT TO DO[1,2,5]

Anti-fraud controls work. Organizations reporting fraud that had controls in place experienced smaller losses and a shorter duration of a fraud episode than organizations without.

KEY FACTOR:

What is important to note is that of the three factors of the Fraud Triangle, reducing or eliminating the opportunity for a person to commit fraud is generally the most effective way to reduce fraud risk. Proactively setting and utilizing controls has proven to make THE difference to protect company performance above all else.

With controls in place, both loss and duration are reduced.[2]

LOSS:
14-54% LOWER

DURATION:
33-50% QUICKER RESOLUTION

REDUCING THE RISK OF FRAUD[5]

Below are some of the types of specific best practices that can prevent fraud and help mitigate risks due to both human and organizational perpetrators:

- Set the "Tone from the Top"
- Separate roles, especially those in: purchasing, A/P, and vendor management
- Scrutinize processes/decisions continually
- Require multiple authorizations on purchases
- Review support documentation before issuing payments
- Perform thorough background checks
- Evaluate code of ethics and policies on fraud
- Look at internal/external audit programs
- Educate audit committee and boards
- Provide and require annual training programs
- Integrate fraud monitoring into an Enterprise Risk Management (ERM) program
- Implement a whistleblower policy
- Discuss SAS 99 with the external auditors
- Deploy technology solutions: Access controls, transaction monitoring, and data access/mining

All of these activities will help to prevent fraud, and they will work best when they become standard elements of your corporate culture. The importance of having transparency about fraud is especially critical, with the expectations for zero tolerance for fraud extending all the way from the C-suite to the copy room (comprehensive collective coverage).

Because the main preventive solution is top to bottom zero tolerance policy, senior management has the primary responsibility for deterring and detecting fraud, working in concert with the board of directors and audit committee and the internal and external auditors.

EXECUTIVES FROM THE VERY HEIGHT OF AN ORGANIZATIONAL CHART MUST HONOR AND REINFORCE POLICY,

including being personally accountable, or the protective policies will be for naught. If those at the top don't take the plan seriously then how can management expect the rest of the employees to adhere to the plan? The tone in any organization is supposed to be set at the top, meaning more than just lip service oversight.

THE SARBANES-OXLEY ACT

Legislation for Strong Governance and Accountability[5]

The Sarbanes-Oxley Act of 2002 was created in response to the major corporate financial reporting scandals in the late 1990s and early 2000s. The Act called for significant reform to public companies' oversight structures and tighter controls around the collaborating accounting firms. In particular, the Act:

Reinforces the responsibility of corporate officers for the accuracy and completeness of corporate financial reports, and adds a requirement for the public certification of each periodic report filed with the SEC that includes financial statements. The chief executive officer and chief financial officer must certify that each such periodic report complies with the requirements of the Securities Exchange Act of 1934 and that the financial statements are fairly presented.

- Establishes criminal penalties for a willful and knowing untrue certification.
- Provides for the disgorgement of the bonuses and profits of executives involved in fraudulent financial reporting.
- Requires evaluations and increased disclosures of a company's internal control over financial reporting by management, and a related report by the external auditor for certain companies.
- Requires other enhanced disclosures, including whether the company has a code of ethics for senior financial officers.
- Enhances the role of the audit committee, including requirements for financial expertise and responsibility for oversight of the company's external auditor.
- Requires companies to establish whistleblower programs, and makes retaliation against whistleblowers unlawful.

These provisions have helped reduce financial reporting fraud and serve as an ongoing deterrent.

In addition, the controls themselves need to be monitored or they can easily be ignored or manipulated, becoming ineffective. Part of a successful anti-fraud program is constant evaluation of an entity's internal and external controls as well as the risk assessment plans and procedures.

THE FINANCIAL REPORTING TEAM

Collaboration is Key

Management, boards of directors, audit committees, internal auditors, and external auditors make up a public company's financial reporting team and have complementary and interconnected roles in delivering high-quality financial reporting to the investing public, including the deterrence and detection of fraud. When the reporting team works together, they can keep the prospect of this hidden problem in the light and mitigating risk and maximizing opportunities for productivity and company performance. These are some of the key factors that contribute to making a fraud risk management program effective:

- A strong, highly ethical tone at the top that permeates the corporate culture.
- Skepticism, a questioning mindset that strengthens professional objectivity, on the part of all participants in the financial reporting supply chain.
- Strong communication among supply chain participants.

To many organizations, especially smaller businesses, planning for, setting up, and maintaining a fraud prevention and detection system may appear challenging. But these steps have the potential to effectively reduce fraud risk and save a business thousands of dollars and, in some cases, their very existence. Compared to the pervasive toll just one incident can take, the risk management protocols can be the strongest investment available to protect company performance.

While each organization must do a cost benefit analysis for their risk management program, research shows that a comprehensive plan that is enforced and monitored can greatly reduce the risk of a fraud being perpetrated at all.

Most frauds go undetected and are uncovered either by accident or as the result of a whistleblower.[2]

Of reported cases:

47.3%
WITH HOTLINE

28.2%
WITHOUT HOTLINE

There are four aspects to address in a quality anti-fraud program.

- ✓ Prevention
- ✓ Detection
- ✓ Response
- ✓ Recovery

PREVENTION

When it comes to limiting the losses associated with occupational fraud, prevention is critical. Fraud prevention measures range from anti-fraud training, reporting programs (whistleblower programs), and hiring policies to "setting the tone from the top," performing risk audits and assessments, and putting in place strong anti-fraud controls are essential in being proactive about risks.

As author and leadership expert Robert Stevenson pointed out in his keynote address at a recent ERM Conference, "If you don't like paying attention to risk, you will hate paying attention to extinction." He emphasized the need to approach risk management beyond just reducing the chance of losses, but rather to ensure the survival of an organization. He emphasized, "Future success is not inevitable because of past triumphs." In other words, waiting until something 'bad' happens is waiting too long.

Prevention begins with an effective compliance program. Typical components of a successful program are: due diligence in the hiring process; clear standards for conduct established at the initial hiring and observed by all with consistency; clear expectations including disciplinary actions for misconduct; periodic assessment of both staff and systems, and fraud specific detection policies.

Further proactive preventions include:

- Fostering a Culture of Awareness
- Requiring Compliance
- Expecting Detection of Incidents
- Zero Tolerance
- Clear Consequences & Disciplinary Action
- Appropriate Oversight
- Regular Periodic Analytical Reviews
- Employee Job or Duty Rotations
- Internal Audits – both routine and surprise.

DETECTION

Detecting fraud can come from a variety of sources, including an internal audit, an internal or external whistleblower, surveillance, or even by accident. The means of detection also correlates closely with the likely loss and resulting recovery. Frauds detected by internal controls or internal audits generally result in far smaller losses than frauds detected by external or reactive measures such as a whistleblower tip. However, the most common source is usually a whistleblower tip from a fellow employee.

TO BE EFFECTIVE, ALL COMPLIANCE PROGRAMS MUST HAVE SOME SYSTEMS IN PLACE FOR REPORTING FRAUD.

The most effective ones include an anonymous hotline or web-based portal for reporting a suspected fraud. While anonymous tips via reporting system or hotline are not necessarily the most effective for prevention, they end up helping the most often of all systems.

- Tips: 39.1%
- Reporting hotlines are more likely to detect fraud through tips than organizations without hotlines
  - 47.3% with hotlines vs. 28.2% without hotlines
- Hotlines are most common (39.5%) but internet reporting is more popular combined (34.1% email; 23.5% online form)

Since most tips come from within, it makes sense to set up an anonymous reporting system that allow employees to do so effectively and without fear of repercussion. These outlets are one of the best guards against fraud. Empowering all levels of staff to be protecting the company can build morale and deepen employee commitment to the company's healthy bottom line.

Internal controls, or a direct reporting system, are also highly effective.

- Report to a direct supervisor: 20.6%
- Report to company execs: 18%

External controls in the form of regular audits and complementary internal/external controls designed to work in collaboration are the other most effective detection systems.

A final factor in detection is direct discovery - whether active or passive. Active discovery, meaning putting methods in place with an expectation of detection, results in lower median loss and durations than detection through passive discovery, which is more happening upon an incident. Active discovery methods include surveillance, monitoring and account reconciliation. Examples of passive discovery methods are police findings or discovery by accident.

RESPONSE / RECOVERY[2,5]

If and when an incident is suspected, a timely, efficient and appropriate investigation is critical. Acting fast and being proactive can not only mitigate the risk but in some cases can even recover losses. Especially if an internal control is the method for detection (whistleblower or direct report), fast action will reinforce the risk management system and further the protective quality of the entire program. Conversely, a slow response or ignoring a suspected threat will deteriorate any anti-fraud program and can send a message that the organization is complacent, potentially even encouraging others to pursue misconduct.

Sadly, more than

40% OF VICTIM ORGANIZATIONS DON'T REPORT MISCONDUCT

for fear of damage to an otherwise respectable reputation. Not reporting, however, can be translated into condoning.

As much as it pays to pay attention, it also pays to report.

81%

OF THE TIME LEGAL ACTION PROCEEDS, THE JUDGEMENT IS AWARDED TO THE VICTIM ORGANIZATION.

In less than 10% of cases is a victim organization fined.

CONCLUSION

Whatever the methods employed, fraud prevention systems are critical to protecting your business. When a program is designed and managed well, internal and external teams can continuously flourish and collectively produce a healthy culture and bottom line. Left hidden or ignored, occupational fraud can quietly drain the profits as well as the resilience of the organization.

Take action today.

Proper planning can help your business avoid becoming a statistic in the next study. If you need help designing an effective fraud prevention program that doesn't let "red flags" go unnoticed, we can help. Request a consultation with a Lowers Risk Group consultant today.

ABOUT LOWERS RISK GROUP

Lowers Risk Group integrates the services of three industry-leading companies – Lowers & Associates, Proforma Screening Solutions, and Wholesale Screening Solutions – to create a complete risk management service offering for any organization. Employed in concert or on a standalone basis, the Lowers Risk Group companies excel in providing comprehensive enterprise risk management and human capital risk solutions to organizations operating in high-risk and highly-regulated environments. Our specialized background screening and crime and fidelity risk mitigation services protect people, brands, and profits from avoidable loss and harm. Our satisfied customers have come to expect and rely upon our experienced and professional approach for their risk assessment, compliance, investigation, claims, due diligence, background screening, and related risk mitigation needs to help them move forward with confidence.

Sources:

1 *2016 ACFE Report to the Nations (RTTN) on Occupational Fraud and Abuse, Global Fraud Study*

2 *Exec Summary from Report / Key Stats*

3 *[Infographic] Staggering Cost of Fraud*

4 *2011 Intro to Fraud Exam*

5 *Center for Audit Quality (CAQ) Deterring Fraud Platform for Action Guide, 2010*

6 *2014 ACFE RTTN*

7 *2012 ACFE RTTN*

8 *Smart CEO: Occupational Fraud is Still a Big Issue*

LowersRiskGroup®

Protecting People, Brands, and Profits

LowersRiskGroup.com | (540) 338-7151