ULTIMATE FRAUD PREVENTION HANDBOOK

Be Fraud Aware

Fraud Can Happen Anywhere

Yes, it can happen to your business. Business owners don't usually notice fraud losses right away because the frauds are typically hidden in various accounts and paperwork. Padding time sheets, inventory theft, billing and payroll schemes, or confiscating receivables are easily hidden inside the books and can remain hidden for quite some time before they are revealed. Most fraud and employee theft comes to the attention of the employer by either an anonymous employee tip, or by accident.

What can you do to reduce the risk of occupational fraud, waste and abuse? The most effective prevention measure is the fear of getting caught. But the longer frauds go unnoticed and nobody is caught, the more damage is done. According to the ACFE's Report to the Nations, the median duration of fraud – the time from when the fraud started until it was detected – is 18 months. That amount of time can do serious damage to a smaller business.

When it comes to smaller businesses, usually weak or non-existent internal controls, or a breakdown in the company's processes can create a prime opportunity for an employee to steal. Inadequate separation of duties, the absence of mandatory vacations, a company constantly in flux with rapid turnover of employees are all examples of opportunities to commit fraud. The best approach is a proactive approach, taking steps to minimize the risk of occupational fraud, waste, and abuse. It may also require a business to think like a thief: "If I were going to steal, how would I do it and not get caught."

Content

Profile of a Fraudster

Performance, processing, reporting and analyzing of data involved humans. And naturally humans make mistakes, have lapses in judgment, and sometimes break the rules. Many organizations have the mindset of "pfft, that could never happen here". But in organizations it's people who deal with processes, financial transactions, numbers, and data.

So what leads people to succumb to pressure, opportunity, and rationalization to commit fraud? It's critical that organizations protect themselves from dishonest employees.

What do these fraudulent people look like? Well like anyone else. You know them as the people you work with, your friends, family members, acquaintances. Outwardly they may appear honest and ethical, which makes it hard to suspect that they could possibly commit such an action. But that's what fraud prevention is all about.

The ACFE's Report to the Nations[1], covering Occupational Fraud and Abuse, gives insight into what a fraudster looks like. The ACFE studied 1483 occupational fraud cases. The following statistics are pulled from their insights:

- 42% were staff-level employees, and 36% were mid-level managers.
- 55% worked alone in committing their scheme
- 52% were between the ages of 31 and 45
- Two-thirds were male
- 47% had worked for the victim organization for less than six years.
- 72% had at least some university education
- 45% worked in the accounting, primary operations, or sales functions of the victim organization
- 87% were first-time offenders with no criminal history of fraudulent behavior
- 44% were known to be living beyond their means

Does that mean that the co-worker sitting next to you who seemingly falls under all these points is going to commit fraud? What organizations can do with this data is use it to provide context and awareness for those who might fit into these higher risk areas.

Fraud perpetrators don't have a fraud sign pinned to their backs. They don't have "fraud" stamped to their foreheads. The more an organization can educate itself about what the human side of fraud looks like, they are better equipped in preventing it.

10 Reasons Good People Commit Fraud

We've seen in the ACFE's Report to the Nations findings that the higher the perpetrator's level of authority, the greater the fraud losses tend to be. It goes to say that many white collar crimes aren't committed by 'hardened criminals', but instead by people who are under severe pressure from management or shareholders.

There's also those who 'get away with it the first time' then try to test their limits going forward. Why would 'normal' people cross the line to commit fraud?[2]

Tunnel Vision

Many of us find ourselves traveling down that path of focusing on only one thing. Setting and achieving goals is important, however, a single-minded focus on those goals can blind people to ethical concerns. When Enron offered large bonuses to employees for bringing in sales, they became so focused on that goal that they forgot to make sure they were profitable or moral. Look where that got Enron!

The Power of Names

The use of nicknames and euphemisms given to questionable practices can often free someone from their moral connotations. This makes those questionable practices seem more acceptable. Example: Bribery becomes 'greasing the wheels', fraud becomes 'financial engineering'. Cute? Sure. Bad? Oh you bet!

Social Bond Theory

In many bigger organizations, employees may start to feel like numbers, rather than individuals. Employees may often feel detached from the company's goals and leadership. That feeling of being detached may be that driving factor that enables employees to commit fraud.

Time Pressure

If given ample time, an employee might think about their actions as being ethical or not. If under a time constraint, many employees may forget about 'thinking about their actions' and just get the job done to please management, ethical or not.

Con't

10 Reasons Good People Commit Fraud

Acceptance of Small Theft

Look at any workplace and you'll find many opportunities for theft. From post-it notes, to toilet paper. These items frequently go home with employees. And these small thefts tend to be ignored. This then feeds to pushing the limits and engaging in larger and larger thefts.

Self-Serving Bias

It's human nature - we often think we're better than the people around us. This can lead to feelings of injustice if, for example, somebody else gets a promotion over you. Employees feel it's not down to that person's performance and capacity, so it must be something else. These feelings, and overestimation of other's biases can lead to unethical behavior.

Obedience to Authority

When someone in a position of authority asks an employee to do something unethical or illegal, that employee often finds it difficult to say no. After all it's upper management doing the asking so it must be okay. When people see themselves doing another's wishes, they feel less responsible.

The Blinding Effect of Power

The only reason powerful people appear more corrupt is because they are caught more publicly. And when someone is influential and sets rules for others, they can begin to see themselves as morally distinct from their employees, and not subject to the same rules.

The Free-Rider Problem

Positive and ethical behavior can sometimes result in an opposite reaction. "If nobody else steals stationary, the company won't notice if I do." If total damage is limited, people feel as though they can take more liberties.

The Foot in the Door

When upper management asks an employee to skirt the rules, that employee may want to seem like a team player, extremely loyal, and getting things done. In that frame of mind, they may be willing to participate in unethical behaviour.

6 Facts About Fraud & the Benefits of Ethics Reporting

Do You Think You're Immune to Fraud? Of Course You're Not! No matter your organization size, fraud will rear its ugly head, it's just a matter of when.

Smaller companies are especially hit harder when fraud strikes, but for those of you who make fraud prevention take a back seat in your business plan, here are 6 facts about fraud supporting why you should consider stepping up your prevention methods.[3]

The #1 Fraud Detection Method is a TIP

More fraud is detected by anonymous employee tips than by all other means combined. While it is important to continue to utilize multiple fraud deterrent methods such as external audits, separation of duties, and fraud awareness training, the most important tool an organization can implement is a confidential reporting hotline.

33% of All Business Failures or Bankruptcies are Due to Theft and Fraud

Because many smaller firms do not have the means or sophistication to implement strong internal controls, the extent of their losses can be devastating for their business. This fact alone makes it even more imperative for smaller operators to have a hotline set up to ensure they can gain access to information earlier to mitigate any potential losses.

43% of all Private Companies Have Reported Experiencing Fraud

The other 57%? Well it might be a matter of time. While public companies are mandated to have a whistleblower system in place and now even more non-profits are implementing these systems as a way to protect reputational and financial risk, private companies who believe they don't need these systems are setting themselves up for potential disaster. Most fraud is conducted by long-term employees who have access to accounting, operations, sales or manufacturing. Private companies need to ensure they put internal controls in place.

Con't

6 Facts About Fraud & the Benefits of Ethics Reporting

The Median Time for Fraud Detection is 18 Months

Just imagine! 18 months is a long time to continually bleed a company. That's a whole year and a half of losing money and/or property due to theft and fraud. It can be devastating and at times non-recoverable for many businesses. The more internal controls a company has in place, the more quickly fraud will be discovered. Employee training, management's commitment to a whistleblower policy and anti-retaliation practices are key to ensuring staff feels confident about coming forward to report wrongdoing sooner.

Small Businesses are Particularly Vulnerable to Fraud

Fraud costs small business a median loss of $155,000, according to the ACFE. Because small businesses are usually focused on the day-to-day operations, strategic planning can often get pushed to another day. Implementing vast internal controls is always best, but for small business, implementing small measures to begin with is a good place to start. Again, setting up a hotline is easy, cost-effective and an instant way to gain access to information that could save your business.

49% of Victim Organizations Do Not Recover Their Losses

Almost half of all victim organizations discover their losses long after they have been spent. Studies show that the majority of business fraud does not go into investment properties or other such recoverable items, rather the perpetrators used it to support lavish lifestyle enhancements and spending, gambling or other addictions. And that's it - the money is gone and good luck recovering it. This statistic is especially concerning as again, with no opportunity to recover the missing funds, 33% of businesses that experience fraud, ultimately fail.

"An effective ethics reporting tool helps support a culture of integrity and responsibility within the workplace."

3 Popular Business Frauds that Don’t Play Nice, and How You Can Prevent Them

The bigger the organization, the more resources are put in place to battle fraud, and the more slush fund there is to pay violations and fines.

And we know that fraud hurts more when you're a smaller business because there just isn’t the resources or funding available to combat it. Fraud costs small business a median loss of $155,000, according to the ACFE. This is just too much for any small business to handle, and this is a huge threat to the success of that small business.

There are a few scams that businesses need to be on the lookout for - these three more popular examples of fraud can affect any business anywhere, any industry, any size. No matter the size of the organization, it is important that all levels of staff be aware of these frequent scams.

Wire Frauds

One type of wire fraud currently targeting businesses is a type of phishing. The potential victim receives an email that appears to come from their employer's human resources or technical support department. Fraudsters create email addresses that mimic that of the real departments. An email message will be sent to the accounting department advising that the "executive" is working off-site and has identified an outstanding payment that needs to be made as soon as possible. The "executive" instructs the payment to be made and provides a name and a bank account where the funds are to be sent. Typical losses can be in excess of $100,000.00.

Here's what you need to know

- Beware of unsolicited emails from individuals or financial institutions presenting an urgent situation requiring immediate attention
- Prior to sending any funds or product, make contact with existing clients in person or by telephone to confirm that the request is legitimate
- Watch for spelling and formatting errors and be wary of clicking on any attachments, they can contain viruses and spyware

Con't

3 Popular Business Frauds that Don't Play Nice, and How You Can Prevent Them

Directory Scams

A business receives an invoice for a directory, publication or listing that they did not order or authorize. Fraudsters will place a call to the business and speak to an employee and ask to confirm details such as the company's address, telephone number and other particulars. An invoice is sent to the company and often payment is made by the accounting department not realizing the company never actually ordered or agreed to pay for the directory. The fraudster may tape record the initial conversation and use that against the company to verify the purchase of the directory.

Here's what you need to know

- Educate employees at every level to be wary of unsolicited calls. Post notices and discuss these scams during staff meetings
- Compile a list of companies that are typically used by your business, give authority to only a number of staff to approve purchases and pay bills
- Fraudsters will use real company names like Yellow Pages to make the invoices seem authentic. Inspect invoices thoroughly prior to making payment

The Supplier Swindle

Businesses can lose significant amounts of money to fraudsters who claim to represent their regular supplier. The scam is targeting businesses that buy supplies from foreign wholesalers and usually involve a spoofed email informing the buyers of a change in payment arrangements. "Email spoofing refers to an email that appears to have originated from one source when it was actually sent from another source." The email notice provides new banking details and requests that future payments be made to this "new" account.

Here's what you need to know

- Beware of unsolicited emails from individuals or financial institutions presenting an urgent situation requiring immediate attention
- Prior to sending any funds or product, make contact with existing clients in person or by telephone to confirm that the request is legitimate
- Watch for spelling and formatting errors and be wary of clicking on any attachments, they can contain viruses and spyware

Fraud Horror Stories That Ought to Scare You to Death

Fraud can happen to your business, and it can happen where you least expect it. Believe it! Organizations world-wide have the potential to lose an estimated 5% of their annual revenues to fraud, according to the ACFE's Report to the Nations. Any small business can suffer theft in the workplace. In fact, one fraud instance can be devastating - the median loss per fraud case in the ACFE's study was $145,000, and more than a fifth of the cases involved losses of at least $1 million.

In smaller businesses, employee camaraderie tends to run deep and these entities know that the cash flow is very important. Every day relies on making bank deposits to keep the business growing, but smaller businesses, don't have the same cash flow to cover fraud losses and theft.

The following two videos from the ACFE highlight the importance for business to be proactive and put systems in place to ensure the work their employees are doing isn't falling under the radar.[4 & 5]

- **Play Video:** Fraud: Yes, it Can Happen to Your Business
- **Play Video:** Too Much Trust: How Fraud Happens Where You Least Expect It

The smallest and simplest of frauds, born out of opportunity and ease, turn into long running episodes costing the business a lot of money - and emotional strain over the breach of trust:

- One employee should not have all the control
- Systems need to be put in place for handling cash
- Deposits should go to a signing authority in the company as another set of eyes

Lessen your vulnerability to fraud:

- Adopt a code of ethics for management and employees and evaluate internal controls for effectiveness. Identify areas of the business that are vulnerable to fraud
- When hiring staff, conduct thorough background investigations
- Educate employees on the warning signs of fraud and fraud prevention techniques
- Implement a hotline. Fraud is still most likely to be detected by a tip. Providing an anonymous reporting system for your employees, contractors and clients will help uncover more fraud
- Communicate regularly to staff about anti-fraud policies, ways to report suspicions of misconduct, and the potential consequences (including termination and prosecution) of fraudulent behavior

How to Improve Fraud Detection in 10 Easy Steps

No organization wants to wake up to find themselves suddenly the center of unexpected liability or unwelcome scrutiny. That vulnerability is more significant with the increase of occupational fraud stimulated by today's tough economy, and your resources are stretched thin.

Fraud costs everyone more if it's ignored, and your organization is not immune from it, no matter what you might think. The ACFE's Report to the Nations on Occupational Fraud and Abuse states that from their study, the median loss caused by fraud was $145,000 - if you're a small business, that could spell disaster. 22% of the cases in the study reported fraud loss of at least $1 million.

Globally...well fraud is a universal problem. Fraud does not discriminate. Any organization, anywhere, anytime.

Here's a quick list of ways to improve your fraud detection - because fraud is not going away:

Use a Hotline

By far, tips are consistently the most common fraud detection technique. The numbers are high - over 40% of fraud cases are detected by a whistleblower tip. This is more than twice the rate of any other detection method. And employees accounted for nearly half of all tips that led to the discovery of fraud.

Multiple Reporting Mechanisms

Offer multiple reporting mechanisms. Your employees aren't the only people with eyes and ears on your organization. Fraud can be observed by contractors, vendors, customers, and members of the public. If your fraud tipsters can access your tip line via phone, email, mail, fax, and web, all parties have different options open to them and they'll be more inclined to choose their method and make their report.

Outsource "Third-Party" Hotline

Internal systems often sit behind firewalls. If you have an internally driven system, there's a good chance employees, who would prefer to use your system from home, can't because they can't access it. An external third-party hotline increases accessibility to anyone who needs to use it.

Con't

How to Improve Fraud Detection in 10 Easy Steps

Training Your Employees

Train all your employees on what fraud is, what to look out for, and how to report it. Frauds will differ from industry to industry. If you're in the healthcare industry, then you need to look out for false billing of services, or incorrect diagnoses reporting. If you're in the financial industry, you'll need to look out for mortgage or securities frauds. If you have a tip hotline, your employees need to know about it and how to use it.

Train Again

A little repetition doesn't hurt. Train your employees often on how and where they can report on any behaviours they think are questionable, and may go against your corporate ethics and culture. – you can never train enough – every opportunity to educate staff on fraud and unethical behaviour is helpful.

Protect Assets

Smaller businesses probably have petty cash funds and other cash assets within the office. Put processes in place for handling these – require receipts for everything. Reconcile your petty cash fund before replenishing it. As well, most organizations require employees to have use of company credit cards. It can be very tempting to misuse these. For example, if you are a manufacturer of a food product, you probably have delivery drivers eating up miles on the road to make their deliveries. The organization will issue credit cards - for use on truck gas, lodging, food, when on the road - that could easily be used for personal vehicle gas-ups, etc. Get receipts for every transaction and compare with on-road schedules.

Fraud Triangle

Most occupational fraudsters exhibit certain behavioural traits that can be warning signs of their crimes. They may be living beyond their means, suddenly owning new houses or cars. Also, they may have unusually close associations with vendors or customers. According to the ACFE, in 92% of fraud cases, at least one common behavioural red flag was detected.

Con't

How to Improve Fraud Detection in 10 Easy Steps

Reduce Opportunity

Internally in your organization, you can help reduce the opportunity for occupational fraud. Sure it's hard today, with a seemingly shrinking workforce, and more work to be done. But if possible with sensitive duties or tasks, try to segregate these between more than one employee. Put internal controls in place to regularly track or audit these sensitive duties. But most important, develop a culture and environment of integrity. An employee is less likely to commit a fraud if they feel like they are a contributing member of the organization, and if management also exhibits actions of integrity and trust.

Spot Audits

By implementing a spot audit program and conducting random audits on particular areas where fraud could occur, you can keep ahead of any possible threat, and if you do find any concerns, you can immediately conduct whatever investigation you need to rectify any issues.

Policies

Having a policy, then filing it away, isn't enough. Your policies need to be kept fresh, updated on occasion, and available organization-wide. These policies will instruct how to manage conduct, ethics and expected behaviour. Important - it has to be actioned from the top down! As well, your policy should cover where and how your employees can report on any concerns they have, and what they can expect as follow-up action when and if they do so.

Fraud can be preventable. You just need to do something about it. Incorporate a strong compliance program that includes an ethics reporting system. And empower your employees to speak up when they see wrongdoing.

5 Steps to Reduce Small Business Fraud

The following are 5 steps small business can take to help reduce occupational fraud and abuse.

Employee Background Checks

You rely on the trust of your employees, but just how much trust is too much. Small business owners and managers wear too many hats resulting in being increasingly distracted from potential misconduct. Most small businesses don't implement fraud detection and prevention strategies until it's too late. Don't just look at skills, but check references of the people you are going to potentially bring into your company and trust with your financials and accounting.

Implement a Written Code of Ethics

It needs to be short, easy to read, and easy to understand. It's tempting to insert much legalese into a document like this, but take a step back and think about exactly who is going to be reading this and why. Is that person going to understand what this document means and why it was created. The Code has to be located within the company where employees can easily access it, or pick it up whenever they want. Most importantly, the document needs to focus on particular ethical challenges that employees will face in that company.

Divide Bookkeeping and Check Signing Authority

There needs to be controls and accountability in place. It's recommended that the person cutting and signing the checks, is not the same person reconciling the accounts. Keep these two functions separated.

Deliver Bank Statements Unopened to Management

If a fraudster knows that bank statements get delivered to management, or to clients, unopened and not tampered with, chances are they will cease the fraud. If a fraudster has the ability to alter statements in any way, or eliminate questionable financial information before they get reviewed by top management or clients, then chances are that fraud will continue, costing both sides considerable money in the long run.

Con't

5 Steps to Reduce Small Business Fraud

Implement a Reporting Mechanism or Hotline

According to the ACFE, the number one method of fraud detection, and prevention, comes from employee tips. Employees are only going to come forward and report what they've seen if they feel protected from retaliation. And this is where a whistleblower program comes into play in business. Businesses that are proactive in their fight against fraud, and incorporate a speak-up culture will find employees coming forward to report on any wrongdoing they see. And this could save a small business a lot of time and money.

The bottom line is that no matter what you may think, any business, any size, is at risk of occupational fraud and abuse. The important thing to remember is that the best way to protect your business against fraud is to be proactive.

Let Employees Blow the Whistle However They Want to

Someone who blows the whistle can be that employee who's the most loyal to the firm - the most energetic employee who's serious about avoiding negative consequences facing their firm from regulators or the law.

When someone takes the time to blow the whistle, they are raising a concern, either in the workplace or externally as a customer or vendor. The whistleblower sees a wrong about to happen, or a danger to someone, or a risk to their organization. Perhaps they see malpractice in how activities are being undertaken, or even a fraud in the workplace. Whistleblowing is an early warning system for misconduct, wrongdoing or dangerous behaviours.

We come across many Codes of Conduct and Whistleblower Policies, and for the most part, the effort that a company has taken to instruct employees on how to report concerns is super. That company has taken time to put into place an avenue for employees to report concerns with instructions written out in their policies.

However, often we come across Codes of Conduct and Whistleblower Policies outlining a company's reporting program, and how employees are to go about blowing the whistle. They very often they go something like this:

... an employee's Supervisor is in the best position to handle areas of misconduct or violations. If you are not comfortable speaking with your Supervisor or you are not satisfied with their response, we encourage you to speak with someone in Human Resources, or another person in management whom you are comfortable approaching. If you are not comfortable speaking with any of these people, you may contact [insert name of board member / C level person here].

This is a great effort and in theory it should work. Many employees would prefer to report areas of misconduct inside the organization rather than taking it to the government or media. But many of these employees would probably not go directly to a supervisor, or at the very least they'd stall before coming forward. That's because when they do come forward, they aren't anonymous. And fear of retaliation is a very real threat.

A National Business Ethics survey[6] found that 1 in 5 whistleblowers experienced retaliation after internally reporting misconduct. And 1 in 3 employees who declined to report a problem pointed to a fear of retribution from senior leadership as the primary reason they didn't bring up any wrongdoing.

Con't

Let Employees Blow the Whistle However They Want to

You have a chance to uncover and address the vast majority of potential issues before media and regulators ever get involved. So let your employees report misconduct anonymously, in a variety of different ways that secure their anonymity. In many cases, employees are completely terrified of reporting a wrong they see. Here's how you can let them do it anonymously:

- Web - anonymous and confidential web reporting keeps an employee's identity under wraps. A third-party web portal that supports different languages enables all employees, to come forward
- Email - many people would prefer to report what they see via email by taking their time to write down an incident. They can step away from reporting, then come back again later
- Hotline - the important thing is that the hotline is answered at all times by a live human being. No employee wants to leave a message especially when they are limited to time and space. With hotlines, speed of answer, ability to recognize the language spoken, source an interpreter, and engage the caller in an investigative and empathetic manner to ensure their comfort is key
- Mail - some people prefer to write out a letter and post it in the mail. It's important to let them do it. It's equally important to have that letter transcribed into the case management system quickly so the investigation process can begin
- Fax - hat enormous piece of equipment lurking in the corner office does get used to receive anonymous reports. Sure it's a dated piece of equipment, but as long as it's plugged in and working, if that's how your employees want to report, then we'll take the report
- 24/7/365 - many employees would rather report a wrong they see from the comfort of their home. If that happens to be at 2:00 AM on a Sunday morning and they decide to call into a hotline, there should be a live person to talk to
- Face to face - this may work for some and it should not be discredited. If you have an employee who's brave enough to go to their supervisor directly and report on a wrong they see, please commend the employee first, before letting them know that you take it seriously and will investigate immediately
- Location - also important to note is that some industries have operations scattered on all corners of the globe. Mining and forestry operations may be limited with their internet connections. Giving these employees many methods to report boosts the chance of reports coming in

Fraud Prevention: Never Too Late for Your Business

The bigger the business, the more employees, and the fraud costs skyrocket. Big businesses that have engaged in fraud end up paying millions in violations, penalties, and legal fees. So why don't they suffer greater from these fines? Because they've got equally prosperous shareholders, business partnerships, investments, and revenue able to cover the costs.

Small and medium sized businesses don't have that kind of cash flow to cover fraud losses, legal fees, and violations. If a smaller business found itself face to face with having to pay fines, cover financial losses, protect its brand and reputation, chances are it is game over for that business.

Smaller businesses do suffer different types of fraud, compared to larger organizations. Where big business might have the financial markets to "play" with and investors to defraud, small business fraud may be more geared towards cooking the books, defrauding vendors, falsifying invoices, etc. And compared to big businesses with many people 'playing the fraud game', all it takes is one bad apple in a small business to wreak havoc and cost the business more money than it has to play with.

Smaller businesses are typically under protected by anti-fraud controls. This makes them considerably more vulnerable to a fraud threat. Resources for anti-fraud controls are limited in many smaller organizations, however, there are measures they can take to fight fraud. Many of these businesses might think that when it comes to fighting fraud in the workplace, the best methods are just too expensive, too high-tech, too complicated, or too hard to set up. Turns out, the best way to fight fraud actually starts with an anonymous employee tip, according the reports from the ACFE.

Are whistleblower hotlines effective? Yes they are.

The ACFE found that in cases where fraud was detected by accident, the fraud lasted an average of 32 months and cost the company around $325,000. But in cases where the fraud was detected through a tip, it lasted around 18 months and only cost $149,000.

More fraud could be detected if organizations harnessed an employee reporting tool. Companies that have an active monitoring program have significantly fewer losses, because they are usually able to catch the crime earlier. So get harnessing this power today - it's never too late.

Summary

The unfortunate fact is that organizations around the world lose an estimated 5% of their annual revenues to fraud.[6]

One single instance of fraud can be devastating to the smaller business as most frauds continue until detection on average for 18 months.

But it is possible to put preventative measures in place to prevent fraud. A few steps can be immediately taken to lessen your vulnerability to fraud:[7]

Be Proactive

Adopt a code of ethics for management and employees. Evaluate your internal controls for effectiveness and identify areas of the business that are vulnerable to fraud.

Establish Hiring Procedures

When hiring employees, conduct background investigations. Check education, credit and employment history as well as references.

Train Employees in Fraud Detection and Prevention

Do employees know the warning signs of fraud? Ensure that all employees know basic fraud detection and prevention tips.

Implement an Anonymous Fraud Hotline

Fraud is still most likely to be detected by a tip. Providing an anonymous reporting system for your employees, contractors and clients will help uncover more fraud.

Increase the Perception of Detection

Communicate regularly to staff about anti-fraud policies, ways to report misconduct, and potential consequences of fraudulent behavior.

Just these tips alone could help prevent your organization from an incident of fraud!

****

1 ACFE 2014 Report to the Nations: http://www.acfe.com/rttn-profile-fraudster.aspx
2 Dr. Muel Kaptein's of the Rotterdam School of Management: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2117396
3 ACFE 2014 Report to the Nations: http://www.acfe.com/rttn-summary.aspx
4 ACFE Fraud Week: http://www.fraudweek.com/Fraud__Yes__It_Can_Happen_to_Your_Business.aspx
5 ACFE Fraud Week: http://www.fraudweek.com/too-much-trust-video.aspx
6 National Business Ethics survey: http://www.ethics.org/downloads/2013NBESFinalWeb.pdf
7 ACFE Fraud Week: http://www.fraudweek.com/uploadedFiles/Fraudweek/content/documents/5%20fraud%20tips.pdf

BUILD AN ETHICAL WORKPLACE

- Comprehensive services provide everything you need to implement your ethics reporting program
- Oversight into your operations, wherever they are in the world
- Limit exposure to risk | protect your organization and your employees
- Certification to ensure your team is educated, protected and secure
- Education to provide tools to support your employees
- Assessment and Consulting to enable you to define your needs for reporting, education and training
- Enhance relationships and encourage transparency within your organization

Anonymous and **confidential** reporting of unethical behaviour, or wrongdoing, **accessible** any where, anytime across your entire organization including vendors and suppliers. **Mitigate** financial & reputational risk. **Minimize** damages and losses.

IntegrityCounts, by WhistleBlower Security offers a simple solution to enhance and encourage an ethical workplace. We have the system and tools to complement existing ethics and compliance programs, all while enhancing employee safety, welfare, wellness, and health.

GET IN TOUCH WITH US!

info@whistleblowersecurity.com | 1-888-921-6875 | www.whistleblowersecurity.com

WHISTLEBLOWER SECURITY

INTEGRITY COUNTS

About WhistleBlower Security

Making Good Companies Better

WhistleBlower Security Inc. was incorporated in 2005 for the parent company, The Walker Group. The Walker Group began in 1968 in the chemical manufacturing sector, where it quickly became an industry leader in product innovation with a focus on environmental sensitivity. Fostering innovation while maintaining a strict policy of environmental responsibility positioned the Walker Group to develop their own in-house code of ethics and conduct, which eventually grew recognition amongst their stakeholders.

With a success history of internal reporting database development as well as a effective corporate ethics policy, it became evident that the Walker Group was well positioned to offer their WhistleBlower Secured™ model to organizations who are seeking to take their operations to the next level.

WhistleBlower Security Inc. is a Canadian based global provider of customized ethics reporting services dedicated to safeguarding businesses against risk, and committed to promoting a culture of integrity, collaboration and transparency for our employees and clients. WhistleBlower's 24/7/365 hotline, reporting and analytic solutions are combined with advanced security and data management to equip organizations with the tangible tools that will deter and prevent ongoing fraud. For more information, visit whistleblowersecurity.com.