Ultimate Fraud Prevention Handbook

External - v1.0

WHISTLEBLOWER SECURITY a Case IQ company

Contents

CHAPTER 1

Fraud Can Happen Anywhere

Business owners don't usually notice fraud losses right away because they are typically hidden inside accounting and other 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 of the time, management only learns of fraud because an employee chose to anonymously report it. Other times it's by pure accident that fraud is stumbled upon.

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 culprits continue their behaviour, the more damage is done. The ACFE's Report to the Nations reports that the median duration of fraud is approximately 14 months until it is detected. That amount of time can do serious damage to many businesses, especially smaller business. We'll cover prevention techniques later on.

When it comes to smaller businesses, usually weak or non-existent internal controls, or a breakdown in the company's processes can create ample opportunity for fraud opportunities. 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 to stopping fraud is a proactive approach to minimize the risk of occupational fraud, waste, and abuse.

Are you aware of your company's fraud risks and how to prevent them?

CHAPTER 2

What Is Fraud?

The easiest way to understand what fraud is, is to think of it as any crime that is committed for personal or business gain, that uses deception as its principal technique. Consequently, fraud includes any intentional or deliberate act to deprive a person or property of money by cunning, deception, or other unfair means.

Types of Fraud

Fraud against an organization can be committed either internally by employees, management or other officers and executives, or externally by customers, vendors, and other parties.

CHAPTER 3

Internal Fraud

Internal fraud is committed by employees, management or other internal stakeholders and is defined by the perpetrator using their occupation for personal enrichment by deliberately misusing the organization's resources, assets, and trust.

Types of Internal Fraud

There are different ways internal stakeholders will commit fraud, but most commonly seen are embezzlement of cash and fraudulent payments.

Embezzlement of Cash

This is fraud involving the misappropriation of cash receipts and falls into two categories - skimming and theft.

Skimming

Skimming is when the fraudster will steal money before it is registered in the accounting system. This form of theft is difficult to detect because the offender leaves no traces behind in the accounting system that internal controls can reveal.

One of the most common examples of skimming systems is the sale of goods or services to a customer where an employee collects the payment from the customer and then retains the money himself without actually registering the sale. Signs of this type of fraud are a loss of gross margin and a shortage of inventory.

Theft

In a more direct approach, theft is when money is already registered, for example in a cash register. This instance of fraud involves the fraudster stealing money immediately after it has been processed, for example stealing cash directly from a cash register immediately after a transaction.

Fraudulent Payments

In this instance of fraud, offenders pay out company money to themselves or to an accomplice who is controlled or has a relationship with the employee. More commonly seen scams in this category are invoice fraud, wage fraud and expense fraud.

Invoice Fraud

This case of fraud has a perpetrator drawing up fraudulent invoices and processing them in the supplier system. Also commonly seen are personal purchases using a company credit card.

Wage Fraud

Here, the fraudster will forge an invoice in order to induce the company to pay a salary to a third party, or ghost employees, who are made to look like they either work for or provide service to the company.

Expense Fraud

In this type of fraud, the fraudster will attempt a reimbursement of expenses, whereby they will manipulate expense reports in order to be reimbursed themselves for a non-commercial expenditure.

External Fraud

External fraud against a company can cover a number of schemes, including dishonest vendors engaging in bid-rigging schemes, billing the company for goods or services not provided, or demanding bribes from employees.

Also seen are instances of dishonest customers submitting bad checks or falsified account information for a payment. As well a common scam is to attempt to return stolen or knock-off products for a refund. In bigger organizations, they may face threats of security breaches and thefts of intellectual property perpetrated by unknown third parties. Other examples of frauds committed by external third-parties include hacking, theft of proprietary information, tax fraud, bankruptcy fraud, insurance fraud, healthcare fraud, and loan fraud.

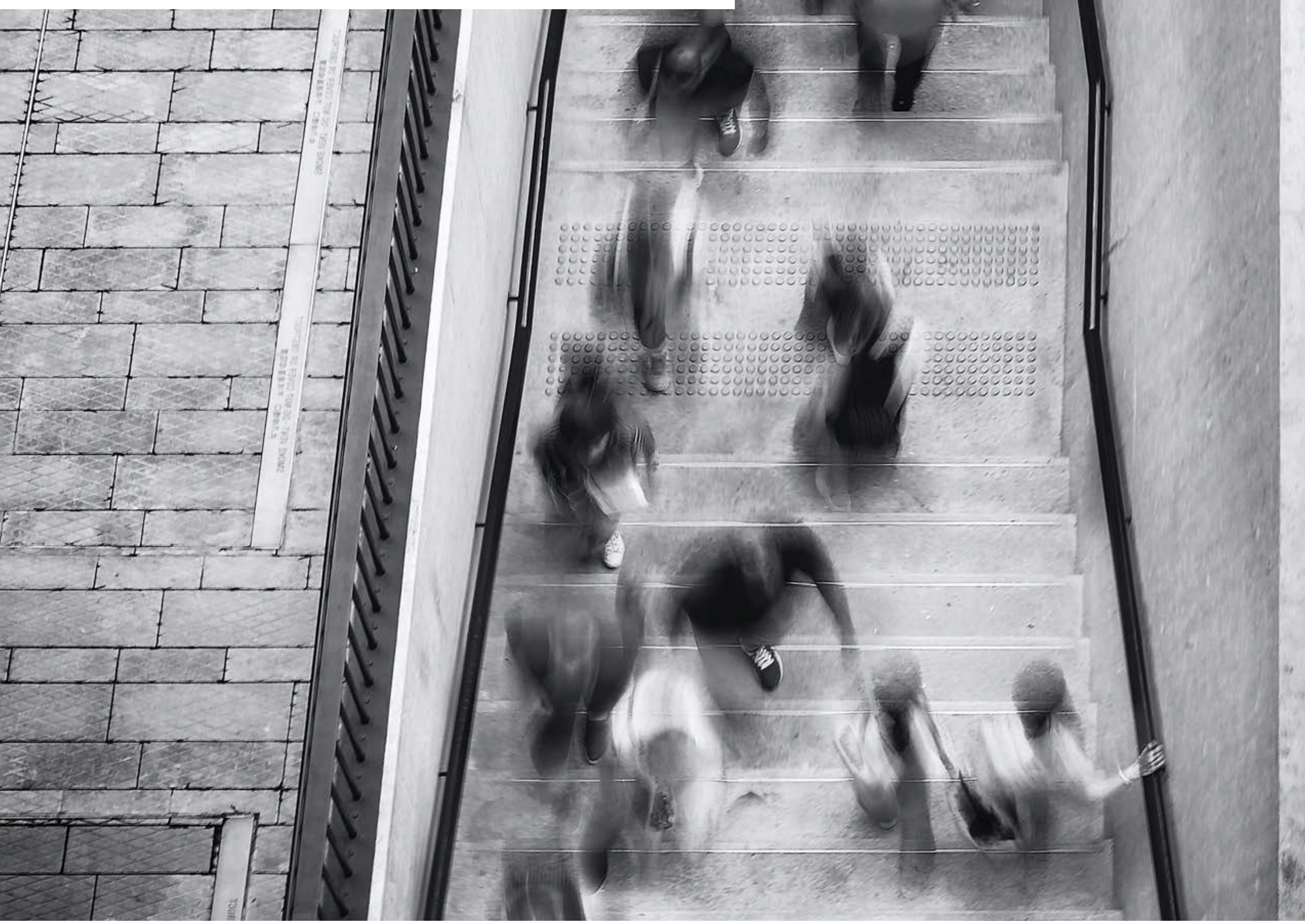
CHAPTER 5

Fraud Against Individuals

Then there is fraud against individuals that many of us have heard of. Many of us know someone who has been a victim of a fraud scheme.

The most commonly seen are identity theft, Ponzi schemes, phishing schemes, and advanced-fee frauds.

These are just a few ways fraudsters will attempt to seal money from unsuspecting victims.



CHAPTER 6

Why Does Fraud Occur?

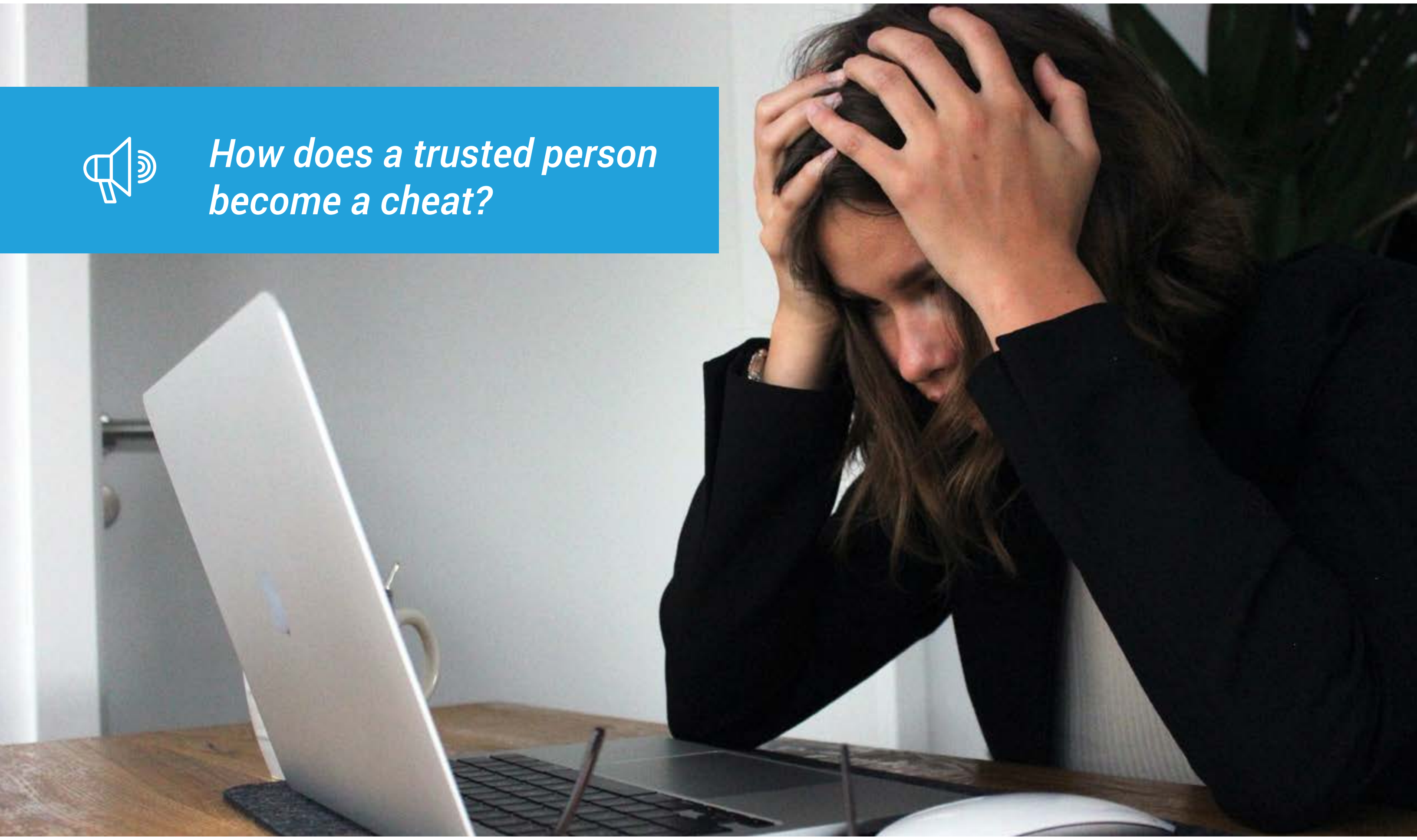
For many fraudsters, if they get away with a crime a first time, they will try a second time, then a third, then a fourth, and so on. With no controls in place, and with the right (and needed) opportunity, a fraudster will strike. And many times, the victims are completely clueless until it's too late.

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. Many white-collar crimes aren't committed by 'hardened criminals', but instead by people who are under severe pressure from management or shareholders.

Do all people do bad things? No. How does a trusted person become a cheat? Most fraudsters are not career criminals. In fact, many would call themselves good citizens who have never committed a fraudulent crime before, until...

And that is the question. What factors led up to that good person committing fraud?

How does a trusted person become a cheat?



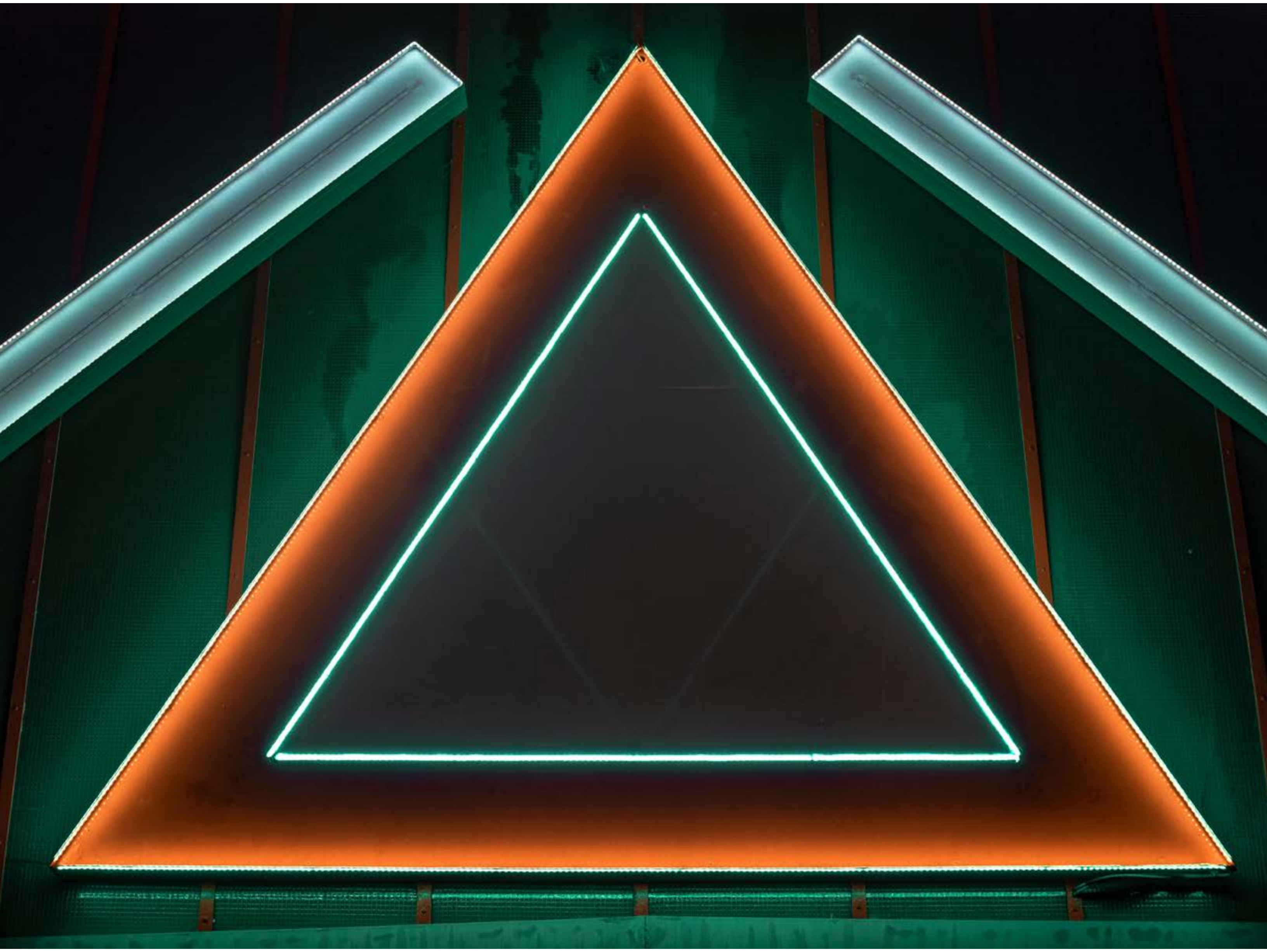
CHAPTER 7

Fraud Triangle

The most widely accepted model for explaining why people commit fraud is the fraud triangle. It is a model developed by Dr. Donald Cressey, an American criminologist who made innovative contributions to the study of organized crime.

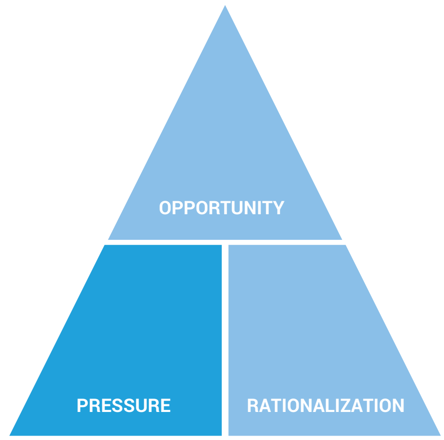
The fraud triangle explains very simply why law-abiding citizens will turn to fraud, and according to Cressey, there are three simple factors: opportunity, pressure and rationalization.

In his model, Cressey explains the three factors that must exist for a normal person to commit fraud:

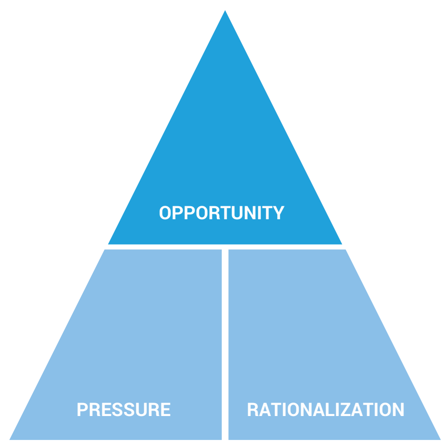


Fraud Triangle

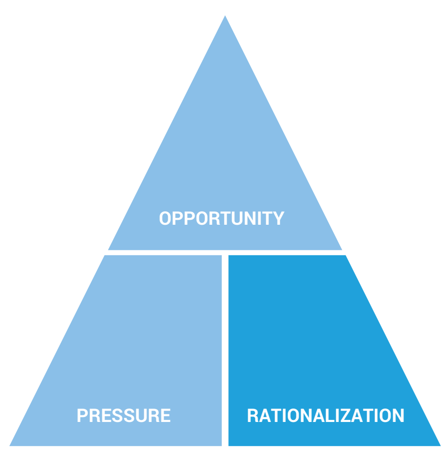
The first part of the triangle is pressure. Pressure is what motivates a crime in the first place. An individual under pressure would be having financial issues, for example, and they are not able to solve their financial problems under normal means. This person would then start to steal small amounts of cash and can move up to falsifying financial statements or creating phantom vendors.



The second piece to the triangle is opportunity. This can be referred to a perceived opportunity whereby the perpetrator commits the crime. If the perpetrator sees an opportunity to better his or her current position, and not get caught, they might try to commit a smaller crime. Critical to this piece is ability for the perpetrator to commit the crime in secret. This could be because they are attempting to maintain a drug problem, or pay off debts from acquiring items they should not be able to afford and they don't want anybody knowing.



The third piece to the triangle is rationalization. Most fraudsters are first time fraudsters with no criminal past and don't see themselves as criminals. They see themselves as good people who happen to be caught in bad circumstances. Because they don't see themselves as criminals, they must justify their actions to themselves. Such justifications can be 'I was only borrowing the money', or 'I was entitled to the money'.



Facts About Fraud

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.

The #1 Fraud Detection Method is a TIP

More fraud is detected by anonymous employee tips than by many other means. 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.

A Third 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.

44% of Private Companies Have Reported Experiencing Fraud

While public companies are mandated to have a whistleblower system in place, now even more private companies and non-profits are implementing these systems as a way to protect against reputational and financial risk. 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.

The Median Time for Fraud Detection is 14 Months

Fraud for this long can devastate companies. It's too long for many to continually bleed money or property due to theft and fraud. Many times it's nonrecoverable for most 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

Certain fraud risks are more prevalent in smaller businesses, like billing fraud, payroll, and cheque and payment tampering. Small businesses, those with fewer than 100 employees have the highest median loss of USD 150,000. Because small businesses are usually focused on the day-to-day operations, strategic planning can often get pushed aside. Implementing internal controls is always best, but for small business, implementing smaller measures to begin with is a good place to start. Setting up a hotline is easy, cost-effective and an instant way to gain access to information that could save your business.

54% of Victim Organizations Do Not Recover Their Losses

About 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. This statistic is especially concerning as with no opportunity to recover the missing funds, a third of victim businesses that experience fraud, ultimately fail.

Impact of Fraud

The devastation from fraud goes well beyond financial losses. Fraud impacts people, companies, services and the environment. When you fully understand the total impact of fraud, companies can then make more informed decisions. Any type of fraud can have a serious impact, whether committed by an opportunistic employee, or an organized crime. Organized crime will, however, increase the scale of destruction.

Human Impact

Fraud is not a victimless crime and is a traumatic experience that causes real and irreversible impacts for victims, families, and communities. Most devastatingly is the harm caused to those who are elderly or vulnerable, who rely on government services. Fraud can have a devastating impact on these victims and increase the disadvantage, vulnerability and inequality they already suffer. Fraud also causes mental and physical trauma for many victims and can result in lost opportunities for many.

Governmental Impact

Fraud weakens a government's ability to deliver services and achieve intended outcomes because money and services are diverted away from those who need it and the services delivered can be substandard or unsafe. This can lead to program failure.

Reputational Impact

Fraud can affect any company, but when handled poorly, it can result in an erosion of trust in government, and leaders, and result in a loss to reputation. This is especially true when fraud is facilitated by corruption.

Environmental impact

Fraud can lead to immediate and long-term environmental damage through pollution and damaged ecosystems and biodiversity. It can also result in significant clean-up costs.

Financial Impact

National-level government entities experience the greatest number of frauds and have the highest median loss. Most of fraud is undetected and can be difficult to categorize. Proactive measures can help entities uncover and more accurately estimate their potential fraud losses.

Business Impact

Certain fraud risks are more prevalent in smaller businesses, and they will feel the impact far more than their larger counterparts. Smaller businesses are far more likely to go out of business due to the impact of fraud.

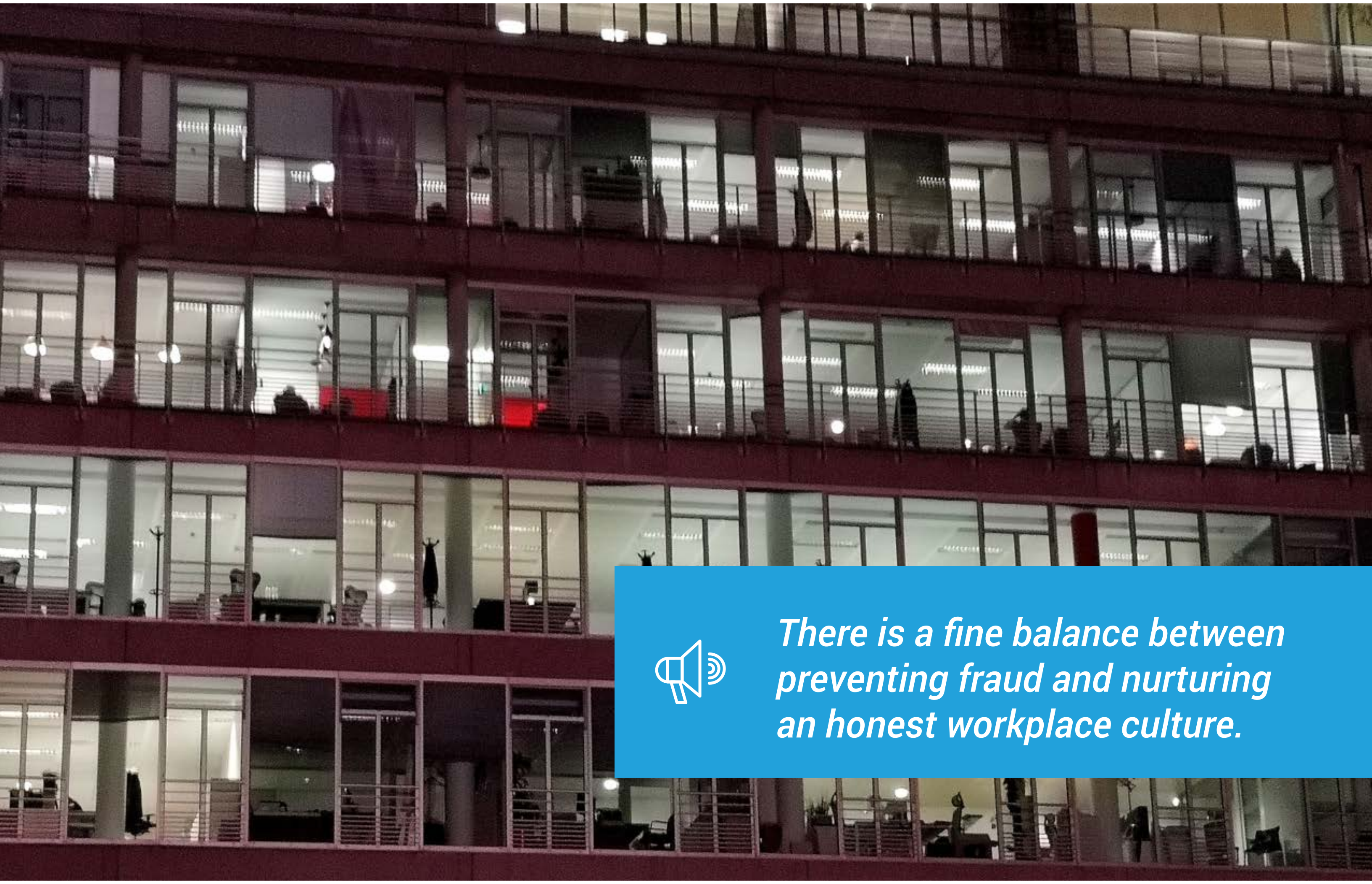
CHAPTER 10

How do I Know if My Business Has Fraud?

It may not always be easy to know right away if your business has a fraud problem. That's because the fraud is being committed by people who you're supposed to trust with your revenue, and assets. And you can't run a business being overly suspicious about your employees and micro-manage them. This is not how a positive workplace culture is created.

At the same time, having strict internal controls in place that every employee must follow does not mean the company is controlling their every move either. There is a fine balance and ways to detect and prevent fraud that offer stringent policies and processes, and at the same time, create and nurture open and honest workplace cultures.

The ACFE's Fraud Prevention Checklist enables organizations to test the effectiveness of their fraud prevention methods.



There is a fine balance between preventing fraud and nurturing an honest workplace culture.

How to Improve Fraud Detection

Training 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 they'll need to look out for false billing of services, or incorrect diagnoses reporting. If you're in the financial industry, they'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.

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 on the road to make their deliveries. The organization will issue credit cards - for use on vehicle gas, lodging, food, when on the road - that could easily be used for personal uses. Get receipts for every transaction and compare with on-road schedules.

Reduce Opportunity

Internally you can help reduce the opportunity for occupational fraud. When it comes to 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 importantly, 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.

Policies

Often times, policies are introduced to employees, then filed away only to be forgotten. 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. Most importantly, they have 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.

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.

CHAPTER 12

Summary

The unfortunate impact of fraud is loss to revenue, reputation and trust. One single instance of fraud can be devastating to smaller businesses the longer it takes place. Prevention measures that are put into place can go a long way to detecting and preventing the destructive nature of fraud.

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 Reporting 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 behaviour.

info@whistleblowersecurity.com

1-888-921-6875

bsi ISO/IEC 27001 Information Security Management CERTIFIED