COMPLIANCE 101

Avoiding Government Investigations and White Collar Crime

Team@ComplianceMitigation.com

Compliance 101

Avoiding Government Investigations and White Collar Crime

Our team at ComplianceMitigation.com helps business leaders and their teams make decisions to avoid government investigations and charges for white-collar crimes.

The Department of Justice encourages business leaders to support well-designed compliance programs that work in practice.

With our compliance programs, your team members will learn how to make better decisions, minimizing vulnerabilties to costly government investigations and charges for white-collar crimes.

Team@ComplianceMitigation.com
949-205-6056

Click to Book Free Consultation

Larry Hartman

Michael Santos

Compliance 101

Avoiding Government Investigations and White Collar Crime

Table of Contents

Why Compliance Training?

Lesson One

Our nation has made a commitment to mass incarceration. We incarcerate more people per capita than any nation on earth. Although most people are intentional when they break laws, many people serve time in state and federal prisons despite not having had any intention to break the law. Rather, they made decisions during the course of business—or life—that brought those people to the attention of government investigators.

Those investigations later led to criminal charges for white-collar crimes.

In an effort to help more people avoid the indignity of being the subject of a government investigation, or the pain of a criminal prosecution, business leaders and the people that comprise business teams should learn about America's criminal justice system and government investigations. Effective compliance training should show business owners and the people with whom they work how and why their decisions on the job can, potentially, lead to government investigations and charges for white-collar crimes.

We all have ideas of what it means to be a best-in-class, successful company. Yet regardless of how successful a company becomes, it's never immune from being taken down by a government investigation. For example, if we ask any group to give us their impression of successful technology companies, we're likely to hear the following names:

» Apple,

» Google,

» Facebook,

» Amazon, and

» Microsoft.

Many of us would consider the above-mentioned companies as models of excellence. They're famous for creating trillions of dollars in value, creating millions of jobs, generating billions of dollars in tax revenues, and providing enormous value to consumers.

Besides being success stories, these companies all share something else in common.

Each of the above-mentioned companies has been the subject of a government investigation. Many people that worked in those companies had to respond to questions from government investigators.

Our team at Compliance Mitigation does not make a judgment call with regard to the reasons behind the investigation, or the usefulness that the investigation would serve. Rather, we want more entrepreneurs, business leaders, and team members to understand how government investigations can threaten businesses and careers. The more a person knows, the more equipped a person becomes to make better decisions—hopefully to avoid being brought in as a witness, a subject, or a target of a government investigation.

From our perspective:

» Business leaders define success by solving problems for customers, bringing value to shareholders, and creating jobs that contribute to vibrant communities.

» Investigators begin their task with a different objective. They believe the company has done something wrong. As such, they will say that they want to get to the truth. But they will define success by obstructing business operations or complicating the lives of business leaders and the entire teams that they target.

Big-government leaders do not limit their attacks to the most successful companies. Elected officials create many government agencies that investigate business operations, business leaders, and people who have decision-making power in businesses. That

means even small companies—and leaders of those companies that have decision-making power—are also vulnerable to government investigations and to charges for white collar crimes.

For that reason, it makes sense for business leaders (and functionaries within each company) to learn about government investigations. That insight can help people involved in businesses both save and make money.

You might ask, "How can investing in compliance help a company or people make more money?"

» Compliance is all about transparency. It's about documenting processes and following best-practice approaches to business. The more companies train people how to follow such procedures, the more effective companies become at messaging. If we communicate well, we're more successful at showing the value proposition we offer.

How does investing in compliance help a company or an individual save more money?

» Investing time and energy to develop effective compliance systems can lead to lower business insurance costs and can lower the enormous risks that business owners and decision makers have to reserve for litigation expenses. Further, they provide insight into business operations and how they might be run more effi-

ciently. Good compliance systems can also lower the risk levels to internal fraud.

Besides saving or making money, investing in ongoing compliance training represents an excellent insurance policy for the company. No company wants to become the subject of a government investigation. The investigations are costly. In many cases, those costs run into the seven figures, both for the business and in many cases, for individuals. Investigations, potentially, can obliterate a business. If authorities bring charges for white-collar crime, they also can lead to loss of liberty for some people.

Evaluation:

In June 2020, the Department of Justice's Criminal Division updated its Evaluation of Corporate Compliance Programs. Essentially, the government white paper offered guidelines for prosecutors to consider when they deliberated over offering leniency, non-prosecution agreements, or deferred-prosecution agreements to businesses. According to the guidance, prosecutors must question the business as follows:

» Is the corporation's compliance program well designed?

» Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?

» Does the corporation's compliance program work in practice?

If we know that prosecutors will ask those questions when assessing a business's compliance program, then business leaders and team members should ask similar questions. By investing time, energy, and resources to understand the importance of compliance, leaders can design a best-practice approach in the design of their compliance training.

Large companies may deploy resources to hire white-glove law firms that specialize in risk management. Those law firms may earn millions of dollars in fees by doing a deep dive to understand a company's operations.

They will perform risk assessments to identify potential problems, assessing the regulatory landscape, the potential clients and the business partners, as well as transactions

with foreign governments, payments to foreign officials, use of third parties, political contributions, and so forth.

Small to mid-size companies may not have the resources to hire such law firms. Yet if they're doing business, their lack of resources will not make them any less vulnerable to investigations and potential prosecution. In fact, those small-to-medium-sized businesses may be easier targets for government investigators.

For this reason, all businesses benefit by helping team members learn more about the real-life consequences that followed for people that lost their liberty as a result of government investigations.

Such training spreads awareness on the collateral consequences that could result from bad decisions made during the course of business.

In making people more aware, our team at Compliance Mitigation can lessen risks for individuals and for businesses that want to show a commitment to minimizing problems with regulators.

Companies that want to minimize risk levels would be prudent to train their team members. As we say at ComplianceMitigation.com:

» We did the time so you won't have to.

Corporate Fraud:

Internal corporate fraud is an ever-growing problem. Government prosecutors bring charges against thousands of people every month for white collar crimes. Those charges leave businesses vulnerable to ongoing problems, including massive legal fees, large fines, and potentially, criminal liabilities.

Management leaders may not have a clear process on how to prevent fraud, or how to respond if they uncover a fraud. We offer this introductory compliance course to assist companies with the following objectives:

1. Help all team members understand the implications of a government investigation,
2. Identify best practices within corporate operations, and encourage employee compliance,
3. Improve messaging and corporate storytelling,
4. Minimize risk to litigation,
5. Teach businesses how to develop a best-practice approach to respond to a government investigation, and
6. Develop a mitigation strategy in the event of a government investigation.

We encourage company leaders to use the modules our team at Compliance Mitigation creates to help all people on

the team understand the costs and collateral consequences of a government investigation. Strength comes through proper preparation.

Members of our team have worked with numerous entrepreneurs that didn't know their business practices violated regulations, or how their policies could expose them to the enormous costs of litigation or a government investigation.

For example, a small business that advertised debt-relief services accepted advance payments from consumers. The business owner hired scores of telemarketers that sold the service. By accepting advance payments from consumers, the business leaders and decisions makers made themselves vulnerable to government investigations. They weren't aware of the Federal Trade Commission's prohibitions against collecting advance fees.

Nor did they understand how a government investigation could lead to:

» litigation,

» an asset freeze, and

» forfeitures that would cripple their business.

Good compliance training helps leaders make better decisions. By investing time to both learn and teach, leaders can create a culture that minimizes exposure to risks in an era of big government.

Larger companies have different complications. People become complacent, expecting that they're operating without risk to regulation or interference from government. Sadly, many rank-and-file employees get dragged into investigations. Their responses to the investigations can bring them into further problems.

Our nation's prison system confines thousands of people that once worked in large companies. Prosecutors convicted those people of white-collar crimes, even though the people professed to be doing their jobs without any knowledge that they were breaking laws.

Although people may begin working in a company with the best of intentions, something can happen during the course of a person's career to throw them off track. Thinking that they could get away with certain actions, some people engage in behavior without fully understanding the consequences.

For example, consider the case of David Smith, who faced charges for crimes he committed while on the job as a manager at Quest Diagnostics.

David faced personal financial problems and, as a result, concocted a complex reimbursement scheme, creating systems that would lead his employer to reimburse him for fraudulent expenses.

Smith created fake companies, invoices, and expense reports for payments he'd supposedly made on Quest's behalf. An internal investigation revealed that Smith had forged his boss's signature. The internal investigation uncovered losses totaling more than $1.2 million. Quest referred the case to the FBI. A judge sentenced Smith to five years in prison. Beside the financial loss and Smith's criminal liability, the distraction undermined confidence in Quest Diagnostic's management team.

Better compliance training serves companies and individuals by:

» Broadening an awareness of the consequences that follow white collar crime,

» Helping people think *before* they compromise their values, and

» Providing transparency into businesses processes, potentially lessening occurrences of internal corporate fraud.

Fraud Triangle:

People like David, in the example above, may not set out to engage in fraudulent behavior but unforeseen circumstances can impact behavior. Educators identify a "Fraud Triangle" that, theoretically, create a perfect storm for fraud. The three corners of the triangle include:

» **Opportunity**: A person like David Smith had to be in the position that would allow him to create the scheme. If he were not in a managerial position, he would not have been able to initiate the scam.

» **Pressure**: David Smith's supervisors may have considered him a competent, trustworthy employee. They may not have known pressures he felt in his personal life.

» **Rationalization**: A person like David Smith may think that the company is so big and profitable that no one would even notice the missing funds.

Although hindsight is 20/20, we can always learn from real case studies:

◊ What if Quest Diagnostics invested more resources in its compliance systems?

◊ What if the training systems included lessons on the high costs of corporate fraud, both for the busi-

ness and for the people that knowingly engage in white-collar crime?

David Smith may have been in a position to commit the fraud, he may have felt pressure, and he may have been able to rationalize his crime.

» The question remains: would better training have convinced him to act with more integrity?

» Would the company benefit by helping more people understand the costs associated with white-collar crimes?

WorldCom and Internal Fraud:

Further consider the example of Walt Pavlo, a person who writes a popular column for *Forbes* online. In January 2001, a federal judge sentenced Walt Pavlo to 41 months in federal prison. The sentence followed Pavlo's conviction for white-collar crimes that included money laundering, wire fraud, and obstruction of justice.

Walt had worked hard to earn an engineering degree and an MBA. Those credentials led to a lead-

ership position at MCI WorldCom, one of the world's most valuable companies at the turn of the century.

In his role as a finance manager, Walt described pressure he felt to report higher revenues than the company earned. The supervisors that oversaw his department wanted to boost WorldCom's financial performance, likely with pressure from the top. When Walt saw that other leaders entered fraudulent transactions, he felt justified to create his own fraud to enrich himself.

Ordinary people may not expect a multi-billion-dollar, global corporation like WorldCom to engage in fraud. Neither would they expect a family man with a professional education to exploit the fraud he discovered—then create his own scam.

Members of our team have met and interacted with thousands of people that served time for white-collar crimes. Despite leading or working with companies that had compliance-training manuals, they did not get the message.

Noncompliance and Fraud:

To make compliance a part of any corporate culture, leaders should include regular training that includes real-life stories. Those stories will help all team members appreciate the magnitude of problems that come with a government investigation. When leaders and team members

grasp the severity of consequences, fewer people will participate in the type of behavior that can increase risk levels for businesses and organizations.

As an added bonus, by investing in compliance training that works, businesses and individuals may qualify for leniency or mitigation in the event that investigators begin asking questions.

It's impossible to predict who might commit fraud within an organization. The vast majority of people that engage in white-collar crime do not have criminal histories. Yet as the theory of the fraud triangle suggests:

» those people may be in a position to commit fraud;

» they may feel pressure that induces them to participate in fraud;

» they may rationalize their behavior for any number of reasons.

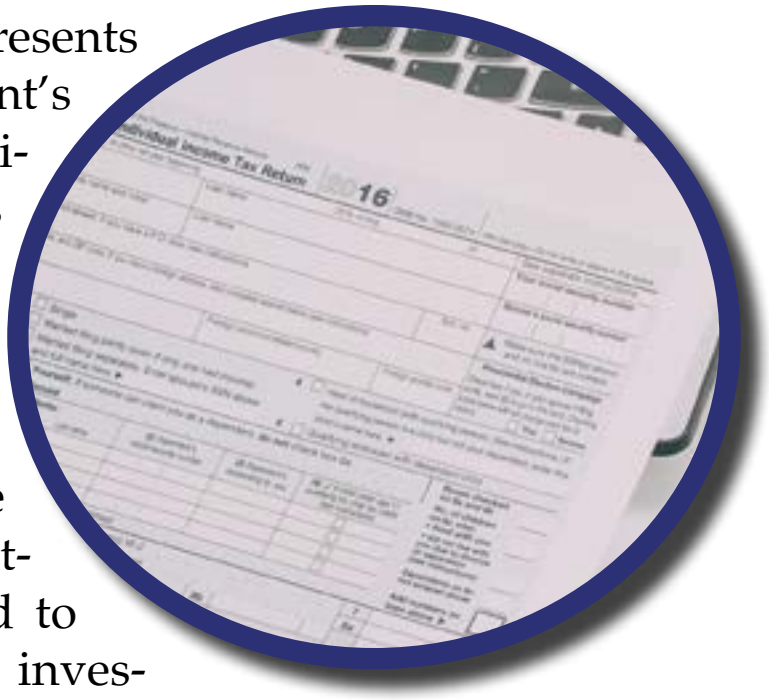
Good training may lower risk levels for businesses and for individuals. Consider statements that our team at Compliance Mitigation found during research for the creation of our course materials:

» According to Carnegie Mellon University's report on Insider Fraud in Financial Services, employees working in accounting, operations, sales, upper manage-

ment, customer service, purchasing, and finance commit 75% of all corporate fraud.

» Employers frequently assume that people always act with integrity, even after being hired. Since businesses incentivize managers to focus on meeting targets and goals rather than detecting fraud, commitment to ongoing compliance training frequently suffers.

» In a report that Intel published, Grand Theft Data, inside sources cause 42% of all company security breaches. Those security breaches can lead to government investigations and litigation, exposing businesses and individuals to enormous levels of stress.



» Corporate fraud represents one of the government's highest criminal priorities. The FBI estimates that white-collar crime costs Americans more than $300 billion annually. Those crimes run the gamut, from accounting schemes designed to deceive management, investors, auditors, and analysts about the true financial condition of a company, to cases involving fraud on the government and insurers, vendors,

and clients. Government agencies scrutinize telemarketers, brokers, crypto currency businesses, cannabis, financial services, and the healthcare field.

» The FBI partners with numerous agencies to capitalize on their experience in specific areas such as securities, taxes, pensions, energy, and commodities. The Bureau has placed greater emphasis on investigating allegations of these frauds, and FBI agents frequently broaden their reach by partnering with other agencies, such as the:

  ◊ Securities and Exchange Commission

  ◊ Commodity Futures Trading Commission

  ◊ Federal Trade Commission

  ◊ Internal Revenue Service

  ◊ Department of Labor

  ◊ Federal Energy Regulatory Commission,

  ◊ US Postal Service

  ◊ Secret Service.

» The Department of Homeland Security has its own independent mandate to criminally pursue fraud, financial crimes involving blackmail, contract fraud, grant

fraud, money laundering, bribery, immigration fraud and program theft.

» Government investigations are likely to increase as a result of COVID-19. The CARES Act, subjects companies to additional scrutiny by establishing three new oversight bodies:

  ◊ the Office of the Special Inspector General for Pandemic Recovery within the Treasury Department;

  ◊ the Pandemic Response Accountability Committee, consisting of the IGs for Departments of Defense, Education, Health and Human Services, Homeland Security, Justice, Labor and the Treasury, among others; and

  ◊ the Congressional Oversight Commission. In fact, dozens of cases have already been brought in connection with abuse of the Payroll Protection Program (PPP).

The Value Proposition

Building a compliance program will protect businesses, shareholders, communities, and individuals. On the surface, the investment may feel like a wasteful expense and hassle. Yet effective compliance programs represent an opportunity to both increase revenues and decrease risk for

debilitating costs. They provide an excellent return with peace-of-mind. As an aside, they may pay for themselves in a variety of ways, including:

- Lowering exposure to fraud, waste, and theft of company assets,
- Creating a more inspiring corporate culture with transparency,
- Reducing insurance costs,
- Opening opportunities for increased efficiencies, and
- Improving internal communications and messaging with prospective customers.

Good compliance metrics may also put a company in a good position for a deferred prosecution agreement (DPA), which may avoid total disruption. Sometimes, the government brings an action but realizes it needs the assistance of the company to prove wrongdoing. For example, federal prosecutors entered into Deferred Prosecution Agreement with Samsung Heavy Industries in 2019. The company agreed to settle matters by paying a fine and cooperating with the government's investigation of bribery. The DPA likely saved millions of dollars for shareholders and may have spared some people from going to prison.

Maintaining compliance equips employees to do their jobs well, reach career goals, and keep customers happy. To paraphrase Warren Buffet:

» It takes five years to grow a reputation, and five minutes to ruin it.

An integrated compliance program becomes a valuable corporate asset. Leverage the compliance training so that people can empower themselves to reach their highest potential. By showing everyone to act in accordance with corporate values, leaders protect the enterprise, the team members, and they increase shareholder value.

What is Corporate Fraud?

Lesson Two

Corporate fraud includes an expansive and growing body of law. Congress and state legislatures create laws with one thing in mind and prosecutors then often utilize those laws in ways never initially envisioned. Federal and state RICO (Racketeer Influenced and Corrupt Organizations Act) statutes serve as perfect examples.

These laws have led to more bureaucratic agencies that promulgate their own regulations totaling millions of pages. Agencies that include the Federal Trade, Commission, the Environmental Protection Agency, the Securities and Exchange Commission, and numerous others search for violations of their regulations.

People may violate these laws and regulations, despite not having knowledge or intent. Unsuspecting individuals and companies often find themselves in the crosshairs of a government investigation and don't even see it coming. Without a proactive plan of legal mitigation, a person can unwarily face severe civil and criminal repercussions.

To understand corporate fraud, we should begin with a basic review of how our nation's founders structured our government. Almost all people that attended school in America remember that we have three separate branches of government:

» **Legislative Branch**: Includes the Senate and the House of Representatives. In these two houses of Congress, legislators pass laws that people in our country must follow. The Congress also controls the country's budget.

» **Executive Branch**: Our president leads the Executive Branch, signing legislative bills into law, and overseeing numerous administrative and law-enforcement agencies to ensure people comply with the laws.

» **Judicial Branch**: The president appoints judges at the district court level to make factual findings, appellate court judges to assess due process in the lower courts, and the Supreme Court, which has the final say over all courts in the United States.

Since we declared our independence, our nation's government has grown. As a result, every individual and every business is subject to following more than 4,500 laws and millions of pages of regulations in the federal system. Besides the federal system, each of our 50 states has its own body of laws. Like the federal government, each state has

many regulatory agencies and law enforcement divisions that enforce compliance.

Despite starting with an intent to create jobs and solve problems for customers, on any given day, business leaders could violate regulations or laws. Sometimes, decisions made in the course of business can lead to civil or criminal investigations. Sadly, investigators can also draw rank-and-file employees into those investigations.

The investigations may start in any number of ways. Ordinarily, they begin in secret. Investigators gather information with hopes of building a case. They may seek documents to review. They may identify people with whom they want to speak:

» As witnesses to a government investigation,

» As subjects to a government investigation, or

» As the target of a government investigation.

Whether a person responds as a witness, a subject, or a target, when people respond to government investigators, they expose themselves to potential liability. Despite not knowing whether they've done anything wrong, people may face civil or criminal charges for corporate fraud, obstruction of justice, or any number of white-collar crimes.

With so much at stake, it makes sense for people to learn as much as possible about government investigations and

how they operate. More knowledge about government investigations will help people make better decisions. In some cases, it makes sense for companies or individuals to hire an experienced white-collar criminal defense lawyer to review compliance programs and get an opinion on levels of exposure to government investigations.

How Do Government Investigations Begin?

Agencies like the Securities and Exchange Commission (SEC) and the Federal Trade Commission (FTC) publish articles on their websites that offer information on how they begin investigations. Those agencies do not hide the fact that investigations begin in secret.

Neither business owners, nor the people that work in the businesses, will know that they're being investigated until the agencies are ready to reveal what they're doing. An agency will not make its case public until the investigative team believes it has the evidence to prevail in the lawsuit or complaint.

Investigators may begin making inquiries for any number of reasons. They may receive a tip, or a complaint. That tip may come from a disgruntled consumer, from a whistleblower, or from a representative at a consumer-protection group, such as the Better Business Bureau. Once the complaint begins, the investigators start working to gather data. If the data suggests that the target has violated regulations, or engaged in corporate fraud, the agency may choose to handle the matter administratively, or it may file a lawsuit in court.

Business owners and employees protect themselves when they understand the power of government investigators. That means, if they're talking over the phone, if they're sending an email, if they're sending a text message, they may want to think about how government investigators would construe their words. The more knowledge a person has about what could happen, the more cautious a person would be when communicating within the organization, or with prospective consumers.

For example, in a case that the Federal Trade Commission was making against a real estate developer that operated a call center, investigators conducted an undercover call. The undercover agents went through the company's process:

» Step 1: They filled out a lead form on the company's website.

» Step 2: They agreed to participate in a telephone pitch at a scheduled time.

» Step 3: They started a recording before the pitch, identifying themselves as agents of the FTC, stating the date, time, and stating that the purpose of the call was to investigate the real estate developer.

» Step 4: The agent's spoke with the developer's representative and asked questions with an intent of gathering evidence to build their case.

» Step 5: After the call, the agents marked the recording into evidence, without the representative ever knowing that she was speaking to a government agency, and that her voice had been recorded and would be used to further a government investigation.

» Step 6: Later, after the FTC filed its lawsuit, the telemarketing sales agent became subjected to a deposition under oath. If investigators believed that the telemarketer had lied, or misled consumers, they could threaten her with either civil or criminal charges.

What is the takeaway from the information above?

As business owners, it's crucial to recognize that government investigators have many resources at their disposal. When they begin investigations, they have an interest in penalizing the company and the individuals that work with the company. Since the agents have authority to con-

duct their investigation in secret, they do not have a duty to let the person know that they're being recorded.

Our team at Compliance Mitigation wants to help both business leaders and team members protect themselves. As citizens, we protect ourselves when we document every stage of our processes. We want to show that we're acting in good faith, because government investigators will always view our decisions from a cynical perspective—exposing people and businesses to sanctions.

In the example of the real estate company, the business could have protected itself by publishing the scripts it creates for telemarketers. Each of those scripts should have been stored on a cloud-based system. Then, the business should invest in training, confirming that each of the telemarketers understood the corporate messaging—messaging that should have been vetted by an attorney who would be knowledgeable about the telemarketing sales rule.

Further, the telemarketers should confirm how often they've been trained to speak in accordance with corporate messaging—and the penalties associated with noncompliance.

Businesses should also train team members on the penalties that follow for those found to have violated agency regulations, rules, or laws.

Legal Exposure

Business leaders may not be trained in law, but ignorance of the law will not shield them from a government investigation. Government investigators will rely upon a doctrine known as *respondeat superior*. The translation from Latin means "Let the master answer." In other words, government agents may hold employers liable for the acts that employees perform during the course of the job.

As an example, we'll offer insight into a case that led to imprisonment for several officers and directors of a publicly traded company. These are people that served time in federal prison, along with members of our team. We have personal knowledge from listening to their stories.

Those people have since been released from prison, and they've gone on to build productive lives. Since the purpose of this exercise is to help our course participants understand the risks, and not to hurt other people, we'll change the names of the people involved.

» Those who want to research the matter may search for the U.S. Securities and Exchange Commission case: CV-03-2834 R (RNZBx) (C.D. Cal.)

While confined at the federal prison camp in Lompoc, a member of our team met James. As a young entrepreneur, he launched an Internet advertising company. James later hired other people to join his company, including Mike, who served as the company's senior vice president of business development, Lisa, who served as the company's vice president of finance, and Cindy, who served as the company's controller and director of finance.

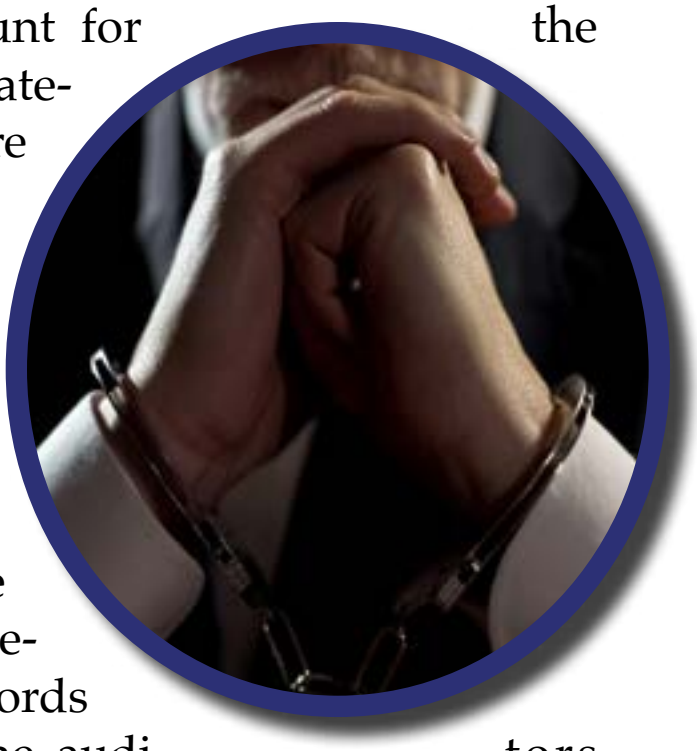
Eventually, investment bankers brought the company public and it performed well during the dawn of the Internet era. Rather than having a background in finance, James's expertise came from selling advertising. He relied upon his team to keep track of records. The company's compensation plan incentivized people to build higher levels of sales, as all of the company's leaders had stock in the company. If the company performed well with growing sales, the stock price would rise. If sales faltered, the company's stock price would drop in the market.

When a recession threatened to slow sales, Mike, Lisa, and Cindy hatched a scheme. They conspired with leaders at another company. Basically, company A agreed to purchase goods and services from company B, and company B agreed to purchase goods and services for the exact same amount from Company A. Company A sent money to com-

pany B, masquerading the transaction as a sale; then, company B sent the exact same amount of money back to company A, masquerading the transaction as a sale.

The sham purchases boosted sales so that investors would think that each company continued bringing in robust sales, even though the conspirators created those sales artificially. In reality, the conspirators understood that those transactions did not represent authentic sales from actual consumers.

As CEO and president of the company, James had direct supervisory authority over Mike, Lisa, and Cindy. James was not on the sales team, nor did he have a finance background. He lacked the requisite skill to understand how Lisa and Cindy would account for the transactions on the financial statements. Nevertheless, James bore responsibility for the actions of the people that worked for him.



Several years later, a larger company made an offer to acquire James's company. During the due diligence phase, forensic accountants researched all of the corporate records of James's company. When the auditors discovered the sham sales transactions, the accountants no-

tified investigators at the Securities and Exchange Commission. Investigators subpoenaed the records, launching a government investigation.

Before the investigators began to ask questions, they had a clear understanding of the deception. Yet neither James, Mike, Cindy, nor Lisa knew that they had been under investigation. When the questions came, they did not know how to respond. Each person lied to the investigators. The people did not know that lying to a federal law enforcement officer exposed each person to a criminal conviction, and the potential for up to five years in federal prison.

As the civil investigation advanced, the agents questioned people as witnesses, as subjects, and as targets. People had to hire lawyers. When prosecutors threatened to bring criminal charges that could expose them to decades in prison, the people began to cooperate in exchange for leniency.

Our team member met both James and Mike in federal prison. Both of them said that had they known the severity of the crime, and the punishments that could follow, they would not have participated.

James and Mike spoke of their perspectives at the time of the crime. When company A purchased a product from company B, and then company A sold a product to company B for the exact same amount, James and Mike believed

that it was a wash. They did not see any harm coming from the transaction.

They did not consider the viewpoint of government regulators or prosecutors. In the eyes of law enforcement, James and Mike participated in a conspiracy to deceive investors. As such, they violated securities laws. By violating laws, they faced a criminal prosecution. With the government investigation and criminal prosecution, they had to spend millions of dollars in attorney fees. Further, they damaged their professional reputations, they lost their liberty, and they have to live as convicted felons.

Questions to Consider:

» As the company's CEO, what level of culpability did James have for the decisions that Mike, Lisa, and Cindy made?

» In what ways would knowledge about criminal penalties influence corporate leaders like James, Mike, Lisa, and Cindy?

» Who would law enforcement officials identify as victims in the case above?

» What type of training could protect a company against decisions like those that James, Mike, Lisa, and Cindy made in the case example above?

During corporate training sessions, it may help for leaders to work through these types of role-playing situations. By helping people understand how government investigations begin, we can go a long way toward helping team members make better decisions. Hopefully, we can also lessen corporate vulnerability to government investigations, and also reduce the number of people that face charges for white-collar crime.

Risk Exposure and Fraud

Lesson Three

Fraud charges can stem from any number of alleged business activities. Corporations exist to earn a profit and maximize shareholder value. Yet regulations make them vulnerable to various ethical rules, such as ones that might damage the environment or harm employees.

When businesses hire people, task them with responsibilities, or interact with consumers, they assume various liabilities. Authorities may charge them with violating regulations or laws that can threaten the business's existence, or liberty for individuals.

Leaders find it impossible to supervise every aspect of an employee's work life or eliminate exposure to fraud or liabilities.

Compliance programs may help team members understand how their decisions can make them or their business vulnerable. By making more team members aware of risk, they may make better decisions, reducing exposure to litigation.

When it comes to limiting exposure from corporate fraud, we can learn from two philosophers, Socrates and Sun Tzu:

» Socrates gave us the wise saying, "Know thyself."

» Sun Tzu followed with the equally wise saying, "Know thy enemy."

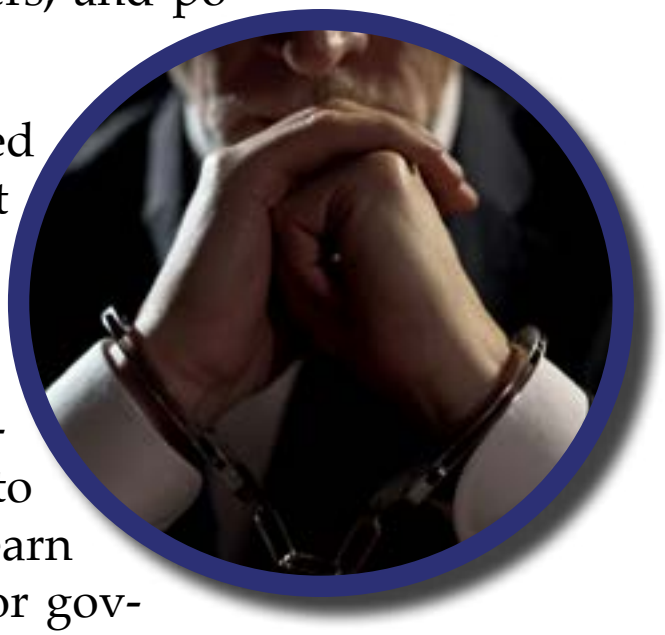
With Socrates, we're taught the importance of introspection. When we reflect upon the connection between our past decisions and our "where we are today," we see relationships. The decisions we made as children opened opportunities for us.

Similarly, decisions we made in early adulthood influenced the careers that we built. As we look forward, we can see the road ahead. Theoretically, that exercise in introspection and contemplation should influence how we think and how we act. Just as the decisions we made yesterday influence where we are today, the decisions that we're making today will influence what we become in the months, years, and decades ahead.

Sun Tzu, author of *The Art of War* taught that in addition to knowing ourself, we also must know our enemy. The more we know about how our enemy thinks, the better we can prepare.

Rather than defining an "enemy" as a human being, we can use the concept of an "enemy" to serve as a framework; besides being a person, an enemy may include a way of thinking, or an action, or a state of affairs that we want to avoid. If we consider "obesity" as an "enemy" of our goal to fitness, we may want to avoid actions that lead to obesity.

As business leaders, we want to avoid litigation and government investigations. That's the enemy. Unless we're lawyers or professionals that earn a living defending against litigation or government investigations, we want to minimize our exposure to activities that could lead to our being deposed, or standing as an "accused" inside of a courtroom. Litigation can bring excessive risks that threaten to undermine our businesses, our careers, and potentially our liberty.



For these reasons, we need to give a great deal of thought to our businesses, our careers, and how our decisions can put those businesses and careers on the pathway to success—or expose us to risks. We also need to think about how people that earn a living from either litigation or government investigations think. The more we know, the better we prepare ourselves to make good decisions, and the

stronger we become at making decisions that can decimate all that we've worked to create.

Two political philosophers, John Locke and Thomas Hobbes, offer us more insight that we can use as we consider risk and mitigation. Thomas Hobbes, author of *Leviathan*, advised on how leaders should govern. At our core, Hobbes believed that as human beings we are basically beasts that fight for survival. To build a society, we need laws to keep people in order. Without strict laws, Hobbes believed that people would act in their own self-interest and to the detriment of the broader society. Enforcement of strict laws keeps people in order.

John Locke, on the other hand, believed that people are rational. We all behave in accordance with what we have learned. At conception, according to Locke, we begin with a blank slate. But every experience makes an impression upon us. Those impressions shape how we think and how we act.

» If we're born into struggle and chaos, we may learn how to adapt in accordance with what we see.

» If we're born in privilege, we act and believe in accordance with what we see.

As rational beings, Locke believed that just as we learned, we could also unlearn.

Unlike Hobbes, who believed that it was the threat of punishment that kept us in line, Locke held that our experiences determine who we are, and what we become. As a society, then, according to Locke, we should invest to help people learn how to behave in ways that advance our communities. Some may consider John Locke as the father of liberalism.

These philosophical understandings are all highly informative in assessing a company's vulnerability to fraud and how to best protect against it.

Philosophy and Risk Management:

Whether we own a business, or we work to earn a paycheck, we all advance when we think as if we're the CEO of our life. And as a CEO, we can rely upon some basic tenets that include:

» Tenet 1: We've got to start by defining success. What are we trying to achieve?

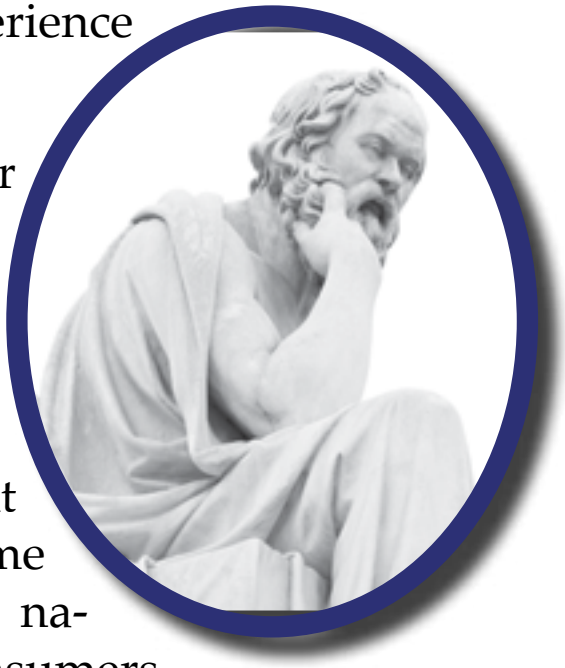
» Tenet 2: We've got to document the strategy that will take us from where we are to where we want to go.

» Tenet 3: We've got to create tools, tactics, and resources that will help us succeed, to achieve that documented strategy.

» Tenet 4: We've got to execute our strategy every day, and we've got to measure our progress.

To use lessons from Sun Tzu, we advance prospects for success when we minimize risks, or exposure to the enemy. To use lessons from Socrates, we need to introspect constantly.

When Socrates said, "*the unexamined life is not worth living*," he advised that we all should make connections between the decisions we're making today, with the potential risks and rewards that we'll experience tomorrow.



We can lessen our risk levels, or our exposure to litigation and government investigations, when we understand the thinking patterns and motivations of regulators—or our opposition.

Like Thomas Hobbes, government regulators believe that if we've come under their purview, we're beasts by nature—out to deceive and defraud consumers, as we prioritize our self-interest. Regulators will define suc-

cess with injunctions, fines, disgorgement, corporate shutdowns, and decimation of businesses.

To lessen risks of litigation and government investigations, our team at Compliance Mitigation helps people understand the various types of corporate fraud; people should have a clear understanding of the exposure that accompanies fraud. Through this lesson, people will learn why a personal investment in compliance and risk-mitigation goes a long way toward advancing prospects for success.

Various Type of Corporate Fraud:

Fraud charges may begin with either civil or criminal investigations; those investigations may stem from any number of alleged activities. An non-exhaustive list of those activities may include:

1. bribery,
2. forgery,
3. copyright and trademark infringement,
4. overbilling,
5. price fixing,
6. embezzlement,

7. insider trading,
8. data theft,
9. unscrupulous telemarketing,
10. money laundering,
11. wire fraud,
12. mail fraud, and
13. deception.

With more than 4,000 criminal statutes, and millions of pages of government regulations, investigators have many more charges at their disposal. Any of those laws or regulations can prompt a government investigation.

For such reasons, business owners do well when they invest time and energy to learn about what happens when investigators bring allegations of fraud. Since the acts of employees can launch an investigation, it makes a lot of sense to include such training for all new hires.

Any decision made during the course of business can threaten to undermine the enterprise.

When business leaders help all members of the company's team understand these concepts, they are better situated to avoid problems that can lead to government investigations or criminal prosecutions.

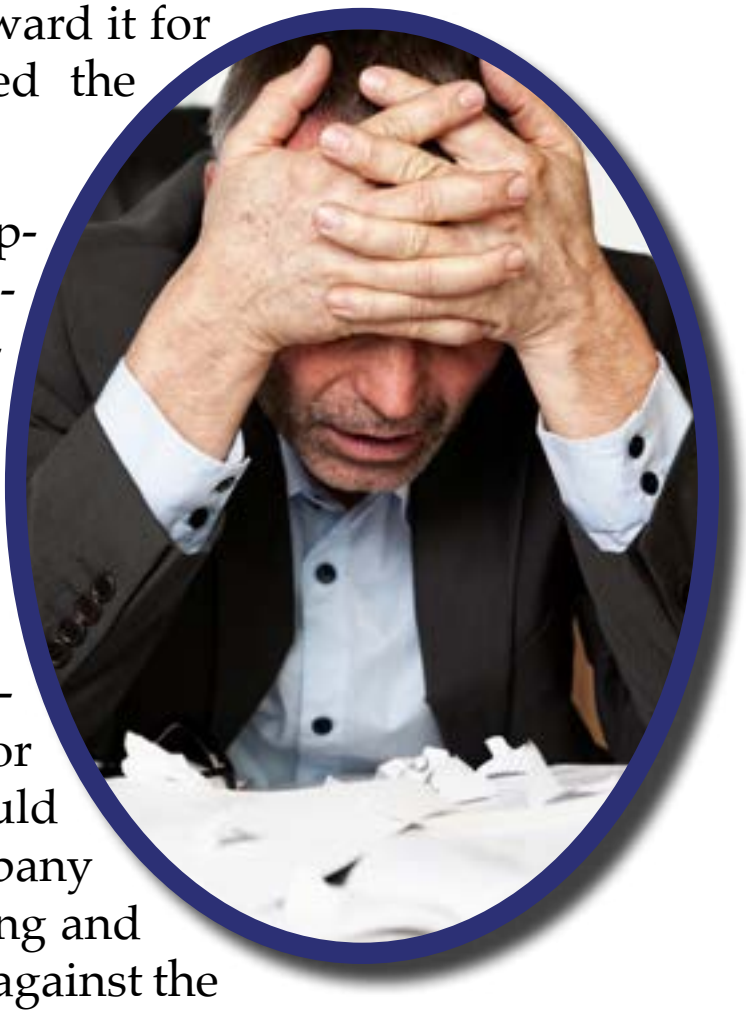
Authorities can charge executives for decisions they made while on the job, and they can also bring charges if people under their control engage in any type of act that they deem nefarious. Those charges can destroy careers, decimate shareholder value, and lead to the loss of liberty.

Even if an individual did not carry out the act, authorities may bring conspiracy charges. With a conspiracy charge, authorities will look to "overt acts" that they believe would further a conspiracy. Conspiracy charges prove to be very useful for prosecutors because they require a lower threshold of proof; further, conspiracy may not require intent, yet they could bring penalties that are identical to those that would exist if the fraud had been consummated directly.

One of the numerous cases brought during this past decade against healthcare providers may be instructive. A director of physical therapy regularly performed services for patients and supervised the services of other therapists, signing approvals for the work of others.

Separately, to further the enterprise, a marketing company (retained by the owners of the healthcare provider and not by the director of physical therapy) orchestrated media campaigns to spread awareness of the business's services. Rather than charging a set fee for its services, the healthcare provider paid the marketing company on a per-patient basis. If the marketing company's efforts resulted in a new patient, the healthcare provider would compensate the marketer.

The government launched an investigation for "patient brokering." Although the marketing company thought its billing approach would reward it for success, legislators deemed the practice illegal.



Patient brokering represents a hot-button topic for regulators. Prosecutors filed charges against many people within the organization. According to prosecutors, the CEO "should have been" better supervising the marketing department. The director of physical therapy "should have known" that the company engaged in patient brokering and that patient brokering was against the law. The marketing company should not have participated.

Each person in the conspiracy bore liability. The director of physical therapy chose to fight the charges at trial. After a jury returned a guilty verdict, the judge sentenced him to 12 years in prison.

For these reasons, stakeholders should understand the nature of corporate fraud and the allegations that may follow from a government investigation. By learning how

regulators attach risk and learning more about the risk-exposure to corporate fraud, we help people make better decisions.

Knowledge can prove an effective first line of defense against any potential exposure.

Common Types of Corporate Fraud

Every company faces unique challenges with respect to fraud, depending on the specific type of business. For example, a chain of pharmacies may not have the same level of exposure to the Foreign Corrupt Protection Act as a steel manufacturer that sells its products around the world.

Nevertheless, in our era of big government, professionals that value their liberty should learn about the various types of fraud, and the risk exposure that accompanies allegations of wrongdoing. Such knowledge, theoretically, will help people make better decisions:

Corporate Account Abuse:

All companies maintain corporate accounts to track transactions. Those corporate accounts may allow employees to order shipments on credit from a supplier; or the company may issue corporate credit cards so that employees don't need to come out of pocket for travel expenses. Managers are often too overwhelmed to extensively review

details, so long as the dollar amounts and types of expenses listed seem reasonable.

Corporate executives may use their corporate accounts to order car services, stay at luxury hotels, take first-class flights, and enjoy other perks while on a business trip. Many think nothing of keeping the frequent flyer miles and hotel points, even though those points technically belong to the company. Some credit-card benefits may include cash-back programs for expenses paid by an employee and reimbursed by the company.

What policies exist to track these transactions? Investigators with the IRS may want to know.

Members of our team served time with an executive that got wrapped up in a government investigation that stemmed from an alleged abuse of expenses. After a prosecution, a judge sentenced him to serve a lengthy term in prison.

If business owners or professionals blur the line with regard to how they account for expenses, they expose the company and their lives to potential civil or criminal liability.

Overbilling:

Overbilling practices can also lead to charges of fraud. For example, we knew the owner of a plumbing supply company that used some of the products in inventory to repair rental properties. He then wrote off the items as business expenses, declaring he lost toilets as being lost due to damage. When a disgruntled employee turned him in to authorities, a government investigation ensued. He went to prison for tax fraud.

Vendor Systems:

Managers should be aware of one of the more common variations of fraud: setting up phantom vendors and creating fraudulent invoices for non-existent goods and services.

This type of fraud requires planning and plotting by the perpetrators, but all managers can get wrapped up in the problem. Investigations that reveal this type of fraud can bring both civil and criminal liability.

Bribery:

Either giving or receiving something in exchange for a purchase order or project can lead to liability.

Regardless of where the bribe takes place, criminal charges can follow. In fact, Oderbrecht, a large Brazilian company paid a $3.5 billion fine in 2016 for bribery that took

place outside of the United States; the CEO went to prison. DOJ prosecutors hold that bribery threatens our national security and the international free market system. And the FBI uses all available resources to both investigate and bring charges for corruption related to bribery.

Smaller independent contractors sometimes feel pressured to offer bribes just to get their foot in the door and keep it there. For example, we knew a former military contractor and West Point graduate that paid a bribe in the form of a "no-show" job to someone instrumental in helping him get a sizable military contract. The contractor, in turn, billed the Army $422,704 for the purported work. After a government investigation, a six-year sentence followed.

Payroll:

A company owner or manager has hiring discretion. Abusing that discretion, however, can lead to charges of corporate fraud. For example, if a company provides employment to a person that does not perform any duties for the business, investigators may allege a fraudulent transaction. The allegation may be that the company took an unfair business expense by providing employment to someone that did not provide any service.

Sales:

If companies try to push revenues into a specific time frame in order to manipulate accounting, investigators may allege fraud. Remember, although we can control what we do, we cannot control what other people do. Accounting scandals can result when people turn their employers in to authorities.

Consider the case of an executive we knew that worked with one of the world's largest software companies. In the years 1998 through 2000, the company began prematurely reporting $3.3 billion in revenues from 363 software contracts, creating what the SEC later facetiously referred to as 35-day months.

Wanting to exceed Wall Street expectations to support the company's rising stock price, the company used accounting trickery. The investigation resulted in the company paying a $225 million settlement; eight people went to prison.

Dating of Documents:

Dozens of companies faced option-backdating scandals, which led to government investigations, fines, huge disruptions within their organizations, and imprisonment for some. Although companies have the right to issue option grants, their accounting practices must comply with regulations to order to withstand the scrutiny of investigations.

Evading Management Supervision:

Telemarketing employees may increase their compensation levels by increasing sales. If not trained properly, however, they may go off-script. When anyone deceives consumers to strike a deal, that person may put the employer, and his or her liberty at risk.

Concerns for Senior Management

Business owners and managers want to increase value with job performance. Similarly, investigators will want to distinguish themselves on the job by building cases that lead to findings of culpability or guilt. With that in mind, leaders should develop an understanding of the following charges that investigators or prosecutors may bring:

Conspiracy:

the company and management can be held liable for conspiracy, regardless of whether the fraud was actually culminated. To prove a conspiracy existed, prosecutors must identify the elements of the offense—like a conversation to deceive consumers.

Then, they must show that the participants engaged in an overt act, like designing a marketing brochure. The deception does not have to take place—only the effort to deceive. Those actions can lead to a conviction for conspir-

acy on any fraud charge, as many people in prison have learned.

Aiding and Abetting:

Sadly, a well-intentioned effort at damage control can lead to charges of a cover-up. We know one person who enjoyed fishing and regularly caught fish without checking or worrying about the limits.

The Coast Guard stopped him for a random check. An officer spotted the captain throwing fish overboard in an attempt to cover up a catch of under-sized fish. The Coast Guard pressured the captain to provide evidence against the owner, or face charges for aiding and abetting.

Investigators may bring charges for aiding and abetting for any number of reasons, including shredding or destroying corporate documents. A good compliance program can shield a leader from such charges, especially if they train regularly on the importance of compliance.

Obstruction of Justice:

When investigators or prosecutors believe that a witness has willfully tried to block the investigation, they may bring charges for obstruction of justice. For example, providing false statements or tampering with or destroying ev-

idence—even before an investigation begins—can lead to criminal charges.

We got a chance to know a media mogul who once controlled the world's third-largest English-language newspaper empire, which published more than 300 newspapers including *The Daily Telegraph* (UK), *Chicago Sun-Times* (U.S.), *The Jerusalem Post* (Israel), *National Post* (Canada). He was world renowned and even anointed a Lord by the Queen of England.

His title didn't keep him from getting charged with 8 counts of fraud for a payment of $5.5 million that allegedly unjustly enriched him. While fighting those charges, he removed 13 boxes of documents from his office, which were merely copies of documents he'd already handed over to the SEC. That action led to additional charges for obstruction of justice. The media mogul appealed and beat the original charges; yet he still had to serve 37 months of the original 78-month sentence because of the obstruction of justice charges.

Responsible Corporate Officer Doctrine:

In some instances management and the company can even be held liable for failure to prevent a wrongful action,

such as in instances of "public welfare" and certain regulatory offenses.

One such instance involved the sale and distribution of tainted eggs and salmonella, leading to criminal liability for the father and son in charge of the company, even though they were not directly involved with day-to-day quality control procedures.

Avoiding Fiduciary Duties:

Honest Services fraud has led many people into the crosshairs of an investigation, and to prison. Politicians and corporate executives perform duties that can be interpreted as favors on any given day.

Voting for a particular bit of legislation, for example, or developing a corporate complex in a specific area. Certain people stand to benefit from these decisions and if any of them can be reverse engineered back to a vote or decision, that can spell potential trouble.

Control Person Liability:

A person who legally controls another person or entity (and it need not be complete control) can be held jointly and severally liable (i.e. responsible for the actions) for the wrongful acts of the controlled person/entity.

We know a former executive of a publicly traded corporation. His company made an acquisition and he delegated material aspects of the merger to several other high-level executives to deal with the details. When the CEO signed and attested to documents filed with the SEC, he exposed himself to criminal liability.

Later, prosecutors charged the CEO and other executives for not recognizing possible warning flags and relying on assurances by subordinates. The government claimed the CEO signed off on financial statements in "reckless disregard" of the truth of their contents. The conviction resulted in a fine of $1 million and a 10-year sentence.

The examples above show the risk exposure for corporate fraud. To minimize exposure to such risks, we encourage regular training on best-practices for compliance at every level of the organization.

Government Investigations

Lesson Four

Government investigations begin much like cancer. They start hidden and slowly, continuing to grow as the individual goes about his or her daily life, unwittingly subject to this dangerous situation. Eventually, the danger becomes apparent.

Detecting the cancer early presents the best chance to lessen the danger. Similarly, if business leaders understand how government investigations begin, they can take steps to minimize exposure to such dangers.

Government investigations typically begin with a complaint from any number of sources. Prosecutors may pressure to bring additional people into the orbit of criminal justice, sometimes coloring the truth in the process.

Our goal at Compliance Mitigation is to guide clients toward best practices in internal fraud prevention, document retention and liability mitigation to help best survive legal scrutiny.

Business leaders and team members should understand how government agencies begin investigations. As discussed in earlier modules, at the start of most investigations, neither business leaders nor front-line staff know that agencies have taken an interest.

Despite a lack of knowledge on the company's part, investigators may be gathering evidence to build a case against the company.

For more insight, we can turn to an article that Mark Eichorn published. In his article, *If the FTC Comes to Call*, Mr. Eichorn, an FTC administrator, wrote:

"All of our investigations are nonpublic. That means we can't disclose whether anyone is the subject of an investigation... FTC staff typically begins with an informal investigation, usually by reviewing publicly available information or even reaching out to the company directly... What we learn may lead us to conduct a full investigation…."

» https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call

Mr. Eichorn's statements, taken directly from the FTC website, confirm that government agencies begin their investigations in secret.

Other readily accessible information lets us know that all government agencies operate in the same, clandestine way. The agencies gather information until they choose to

file a case. By the time an agency files a case, the investigators have an abundance of evidence that they believe will allow them to prevail in a lawsuit. They may sue the company, or they may bring charges against people that work in the company.

Leaders of the Securities and Exchange Commission reveal that they begin investigations in the same way as the FTC. SEC investigators may notice unusual trading activity on public exchanges, or something in the media may perk their interest. Another pathway to an investigation may start with a whistleblower-type complaint from a customer or from an employee who wants to cash in on a reward that follows a settlement.

Any of those scenarios could lead to a government investigation. The target of the investigation may not know about the investigation until the day of a subpoena, raid, or arrest. By that time, the agency will have gathered mountains of evidence.

If an investigative agent or officer of a government agency gets a hint of potential illegal activity, either by a whistle-blower, via another active case, or through various data mining techniques, the agent will begin to investigate further. Once an investigation begins, investigators within the agency, together with government attorneys, will decide whether or not to proceed. If they choose to proceed, they may identify witnesses, subjects, or targets. None of those

people will typically be aware that government officials have begun making inquiries.

Business owners would be wise to remember that government investigators advance their careers by bringing people or businesses down. An investigator's motivation may influence the way he or she perceives business operations. Investigators tend to view evidence from a light that is unfavorable to the business or target.

Once government investigators identify a potential witness, subject, or target, they accumulate evidence that will sustain a finding of guilt. They do not look for evidence that will exonerate a person.

Our team at Compliance Mitigation has come to experience that when investigators find evidence that would weaken an investigator's case, the agents may seek to overlook it. For these reasons, we encourage people to keep accurate records that will exonerate them, or mitigate the charges that may come.

Like sales leaders train their teams to overcome objections, investigative teams train their staff to look at all evidence with a suspicious eye. Unethical government investigators may even try to hide exculpatory evidence. As we've stated previously, all business leaders should remember the perspective, or framework that investigators bring to their work:

» A government investigator prepares for promotions by identifying deception, or noncompliance with regulations. With the growth of our government, legislators and administrative agencies have many laws and regulations that lead to fines, injunctions, disgorgement, and potentially criminal prosecutions. Investigators advance their careers when they find wrongdoing.

For these reasons, every team member grows stronger with a better understanding of how to comply with regulations. That compliance training will help a business save the enormous expenditure of defending against a government investigation.

Further, the investment of time and energy into compliance training will help all team members become more profitable. When they communicate with coherent messaging, every person becomes "*unconsciously conscious*" about how to define excellence within every role in the company; they inherently know how to do the right thing, every time.

Good compliance brings numerous benefits to business owners. On the surface, comprehensive compliance leads to more effective internal fraud-prevention systems. Compliance systems can, however, also greatly improve document retention, thereby protecting the business in the event of a government investigation. Effective mitigation strategies should also help to shield business owners and team members from legal scrutiny.

The Investigative Phase:

To help business leaders appreciate the need for a compliance strategy and ongoing training, our team at Compliance Mitigation created this lesson to teach how investigations evolve. Generally speaking, many investigations begin with some type of complaint. As stated earlier, the complaint may come from disgruntled customers, competitors, suppliers, or the business community.

Employees, too, may alert government officials to what they perceive as wrongdoing by acting as internal whistleblowers. They may even file civil whistleblower lawsuits, also known as *qui tem* cases, going after the massive rewards that result from successful whistleblower lawsuits. In that sense, investigators and aggressive lawyers consider employers as lead-generators that can bring, potentially, massive fines and billable hours.

In the macro sense, we know that high-pressure prosecutorial tactics lead to many government investigations. With our nation's commitment to mass incarceration,

investigators feed the ecosystem that leads to more prosecutions and builds population levels in prison.

Every year, our nation spends more than $100 billion to fill our nation's jails and prisons. To keep them full, investigators work to bring charges against more people and businesses for white-collar crimes. Although some people have a criminal mindset and begin businesses with an intent to deceive or defraud victims, many people commit "crimes" without any intention or knowledge that they are violating laws. For example, the crime of cash structuring has led many people to prison, despite those people not having had any intent to break the law.

Cash structuring makes it a federal crime for any person to make cash deposits in certain circumstances. If prosecutors can prove that a person made a series of deposits that were under $10,000 for the specific purpose of evading the requirement to file a currency transaction report (whether that was actually the intent or not), the prosecutors may bring criminal charges for cash structuring.

As an example, let's say a car dealer sells cars for $9,000. Let's say that the car dealer sold five cars each day. Each time he sold the car, he brought the money to the bank and made a deposit. If the person filled out a currency transaction report, the person would be in compliance with the law—even though he did not deposit $10,000. If the person did not complete the cash transaction report, that individual could be liable for a felony conviction, because author-

ities may accuse him of making a pattern of deposits that amount to less than $10,000 in order to avoid completing a cash-transaction report.

The person in the example above did not intend to violate the law. He completed an invoice system and he paid appropriate tax. The money lawfully belonged to him. Yet as a result of his failure to complete the necessary cash transaction report, prosecutors could bring felony charges; a judge could sentence him to prison. Members of our team have served time in prison alongside several people because they violated cash structuring laws. Those people did not intend on violating the law; they did not know laws restricted the way they could access or deposit their money.

In the law-and-order system of the United States, investigators have massive power. They may question individuals and government attorneys may depose them under oath.

The answers those witnesses give during government investigations can lead to further problems. Government investigators may incentivize people to talk by offering immunity in exchange for testimony, thereby putting more people under scrutiny and bringing more people into the system.

A hypothetical example may help to illustrate how a government investigation can begin. Let's say a policeman pulls a car over for erratic driving. The person driving the

car may be a professional of some sort, a physician, for example. The physician may be driving under the influence.

Understanding that driving while intoxicated could threaten his license to practice medicine, the doctor may request to speak with a detective. The doctor may offer evidence of a fraudulent billing system to overcharge insurers. The detective may have authority to drop the driving offense in order to secure the physician's cooperation if the physician would help to build a bigger case against someone else. The threat of punishment, or loss of earnings, leads many people to become government informants that launch new investigations.

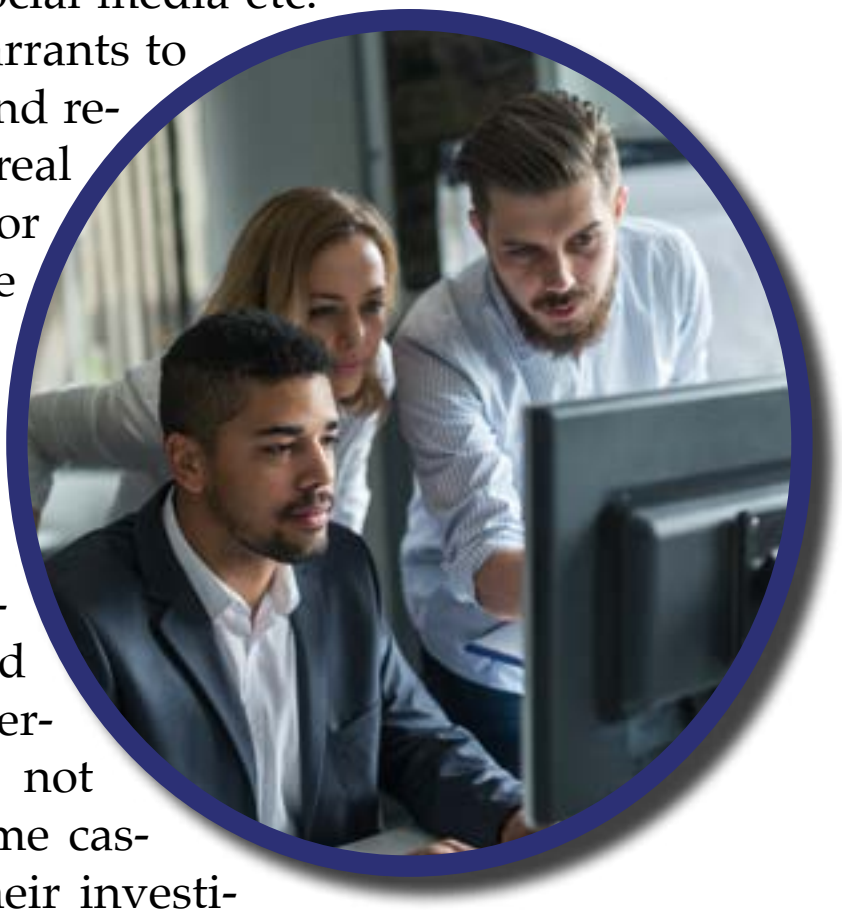
Investigators with various government agencies, including the FBI, the SEC, the FTC, the DHS, the ICE, or any other agency will make an initial determination on whether to advance the investigation.

They may choose to proceed with a civil investigation, or they may work with law enforcement to launch a criminal investigation. Agencies have the authority to conduct civil investigations on their own. Criminal investigations, however, require prosecutors; those prosecutors may work with either with the US Attorney's Office, or with the state Attorney General's office.

Both civil and criminal investigations bring enormous pressure on a person. Every person on our team at Compliance Mitigation has personal experience with those investi-

gations and the consequences that follow. A case may begin with a civil investigation. As evidence surfaces, the investigation may turn criminal, which brings more stress, more expense, and higher levels of risk.

Once investigators choose to advance, they begin to subpoena documents related to the suspected activity. They may want to review bank and brokerage accounts, phone records, email records, social media etc. They can also request warrants to listen in on phone calls and review electronic activity in real time. Again, targets may or may not know that they're being investigated.



Investigators typically do not want a potential target to know anything about the investigation at the outset and will ask people they interview to be discreet and not mention anything. In some cases, investigators make their investigations obvious. They may want to push the target to act inappropriately, while the investigators gain or create additional evidence or charges.

At some point, a target becomes aware or suspicious that an investigation is underway. Whether investigators identify a person as a potential witness, subject, or target, the person would be well advised to understand his or her options. People can take specific actions to minimize potential exposure.

The primary focus during the preliminary phase of a white-collar crime investigation is "what was done" and not "who did it." The earlier a person can persuade investigators or prosecutors that a crime did not take place, the more likely a person would be to get a better outcome.

As investigators and prosecutors spend more time on a case, they become more vested in getting the "win," which doesn't always equate with justice. They want a finding of guilt.

The Prosecution Phase:

If an investigative team feels it has sufficient evidence, then the government agency will bring public charges. In civil investigations, the agency may bring either an administrative proceeding, or it may file a lawsuit in federal court. With criminal charges, the prosecutor may file a criminal information or complaint.

Prosecutors may also convene a grand jury. In a grand jury, the prosecutors present evidence to members of the

grand jury, then request those members to indict the person or the company.

In either civil or criminal investigations, investigators may request a judge to issue a search warrant to raid a person's home or place of business. Citizens should expect that investigators will seize everything possible to help them build a case. They will take computers, cell phones, and all paper records that the warrant authorizes. The investigation will result in significant disruption to a person's life; it could also obliterate prospects to continue business operations.

Later, government lawyers will schedule interviews and depositions. They will subpoena bank records and question third parties. They do not spare any expense in gathering evidence that will help them build a case. In order to lessen exposure to risk, many people within the organization will offer evidence to assist the investigation—sometimes crawling deeper into an investigative trap.

Investigators typically coordinate a strategy to undermine the business and personal life at every level. Remember the nature of a government investigator. Perhaps an analogy is in order. I'll paraphrase an analogy from Aesop's Fables:

The scorpion wants to cross to the other side of the river, but it does not know how to make it across. When the scorpion sees an otter in the water, it requests to ride across the river on the otter's back.

The otter responds, "but if I let you get on my back, you'll sting me and I will die."

The scorpion responds, "why would I do that? I am asking you to help me."

The otter agrees and transports the scorpion across the river. Just before the scorpion climbs off the otter's back, the scorpion stings the otter.

The otter whimpers, "But why did you sting me? I helped you by bringing you to the other side of the river. Now I'm going to die."

The scorpion responds, "It's in my nature."

Remember that it's in the nature of everyone on the investigative team to convict people and businesses. People that build careers as government investigators want high profile convictions.

For this reason, business leaders and team members should adhere to best practices at all times.

Recommendation:

1. Create comprehensive policies that will keep the business and the team members free from the prying eyes of government investigators.

2. Keep accurate records and keep backup materials in cloud-based systems so they are always protected.

3. Create a well-documented process map to show the reasons behind every decision in the business.

4. Train the team members relentlessly.

5. Hire third-party auditors with appropriate levels of expertise to review corporate processes.

Some of the fallout from a government investigation includes reputational damage. Local and potentially national media will offer salacious details, fed by investigators. Internet searches may place a government's press release at the top of a search result. Such reputational damage can lead to enormous complications for a business, and for the individuals identified in the media report. Blogs and posting boards may follow, leading to further stress.

A government investigation will likely lead to the loss of clients, business associates, and abandonment from friends. To avoid being tainted by the investigation, people will scatter and sever ties.

Our team has numerous examples that show how government investigators will taint unrelated parties. We know of a medical office that terminated a woman's employment because authorities brought an indictment against her husband; investigators did not allege that she had anything to do with the crime.

Investigators will use every tool in their arsenal to pressure people to cooperate with an investigation. As a result of their Grand Inquisitor tactics, collateral damage will follow.

Much like business owners crave favorable press for the services they provide, investigators welcome the shock and awe of a well-publicized investigation. For this reason, they frequently favor:

1. the pre-dawn raid at a target's home, with dozens of agents sporting massive firepower, and

2. the blitzkrieg arrest at a corporate headquarters, where scores of agents will come in with windbreakers emblazoned with branding of the government agency.

Investigators do not reserve such tactics for big-time drug dealers, Wall Street titans, or political stars. They use such aggressive tactics routinely, for strategic reasons. Investigators want targets to act irrationally. They want people to protest innocence, or to lie.

Although the target may be new to the proceeding, the investigator knows and understands that with a show of force, some people will lie to the investigators. When those people lie to a law-enforcement officer, they commit a federal criminal offense, under Title 18 of the United States Code, Section 1001. Investigators will use those lies as leverage, threatening imprisonment and other problems, to induce further cooperation.

The more people know, the better people can prepare. Our team at Compliance Mitigation will help you.

Signs of Investigations

Lesson Five

While government investigations begin covertly, they leave clues. Don't ignore the signs. Create good compliance programs that question whether the business and the team members operate in accordance with rules and regulations. When signs suggest that something is wrong, take action to minimize exposure to damage.

Out of an abundance of caution, banks and brokerage firms may cut ties with a business or individual if they're questioned by authorities. They do not want to incur the expense of responding to investigations. Business leaders must be on the alert for any sign that authorities are asking questions that could undermine the company.

A strong compliance program minimizes exposure to investigations. The sooner a business can document a good-faith strategy to operate in compliance with laws and regulations, the better the business positions itself for leniency in the event of an investigation.

What are some of the early signs that a government agency has launched an investigation? Subtle clues may surface. For example, a trusted friend or colleague may start asking questions, or sending emails that detail criminal acts.

Those inquiries may be fishing expeditions, or an effort to get incriminating evidence, like an admission of complicity in wrongdoing. It's important to understand that, in many cases, informants help to expand government investigations by providing information, hoping to lessen their own exposure to culpability.

Investigators want to learn as much as possible, and they want to bring as many people as possible into the investigation. By questioning people as either witnesses, subjects, or targets,

investigators gather information to build cases. In most instances, investigators urge witnesses to be discrete if they're seeking to advance possibilities for leniency.

Besides going after witnesses that provide information, investigators may also seek cooperation from financial institutions. Those questions can, and often do, lead to account closures without an explanation. Although a small business owner may be oblivious to the costs of a government investigation, financial institutions have a deep bench of lawyers on staff, keeping an eye out for the institutions' interests.

All corporate leaders want to mitigate risk that can lead to damages against a firm. Executives in a financial institution, therefore, may elect to sever ties with an account holder if they learn of a government investigation. They do not want investigators dragging them into depositions or inquiries.

Consider, for example, the problems and expense that Deutsche Bank experienced as a result of the endless government investigations into the byzantine finances of President Donald Trump. Every member of our team at Compliance Mitigation can offer insight into the ways that financial institutions will close accounts after they learn of a government investigation.

In anticipation of disruptions to both personal and business accounts, anyone that owns a company or works in a company should develop a best-practice compliance guide to help avoid the disruptions that a government investigation can bring. Executives and employees must also be aware of, and prepared for, the steps to take when they suspect a government investigation might already be underway.

Watch for Red Flags:

At Compliance Mitigation, our team members served time alongside thousands of people that suffered the pains of a government investigation; we've all gone through in-

vestigations ourselves. We can reflect on the red flags we missed along the way. Had we understood the implications of those warnings, we could have taken precautions to minimize exposure.

For example, investigators approached the former CEO and Chairman of a Nasdaq 100 company for questioning. When the CEO called his general counsel, the lawyer told him that it would be fine to speak with the investigators alone, as the CEO didn't have anything to hide. Later, through legal proceedings, the CEO learned that investigators had carved out a special deal for the general counsel; the lawyer served up the CEO as "a bigger fish" to satisfy the government's lust for a headline-grabbing investigation and prosecution.

The markets use many metrics to assess the performance of a CEO. Markets may look at revenue growth, profit growth, and market share. Investigative teams, though, work by an entirely different set of metrics. They advance their careers by bringing people and businesses down. Such motivations influence them to go after cases that generate headlines. Later, investigators and government attorneys rely

upon such results as evidence of their value when advancing their career in government or as they transition to the private sector.

Long before an indictment comes down, investigators leave clues. It's crucial for all parties to keep their eyes wide open. Neither business leaders nor team members should minimize the complexities of a government investigation, including enormous levels of personal stress. The potential for exposure to criminal charges, injunctions, and enormous expenses can lead to total devastation for those that do not have a plan.

Marathon Levels of Stress:

Investigations typically play out over many years. The uncertainty disrupts business operations and obliterates personal sanity. The targets of a government investigation may feel powerless and helpless.

As a precautionary measure, leaders should engineer compliance programs to protect against such disruptions. Regular training should help people understand how doing their job correctly will minimize exposure to investigations and charges for white-collar crimes.

Based on our experience, we recommend that business owners use a solid plan to prepare, at the soonest possible time. For example:

Step 1:

» Create documents that clearly show how the organization defines success.

Step 2:

» Create documents that lay out a step-by-step plan, detailing every aspect of the organization. On a regular basis, preferably quarterly, but at least annually, revisit the plan and make adjustments.

Step 3:

» Create tools, tactics, and resources to articulate precisely how the organization functions and allocates resources. Show the investment that the corporation makes to train all staff members, and to communicate the message to all vendors and consumers. Build a system to organize how the corporation keeps records, with effective backup plans.

Step 4:

» Show the steps the corporation takes to measure progress. Make sure that each team member is aware of the

documentation, and schedule periodic training to refine best practices.

Leaders should take defensive measures to protect the business and all team members, knowing that investigations begin in secret and can occur at any time.

PRE-EMPTIVE MEASURES

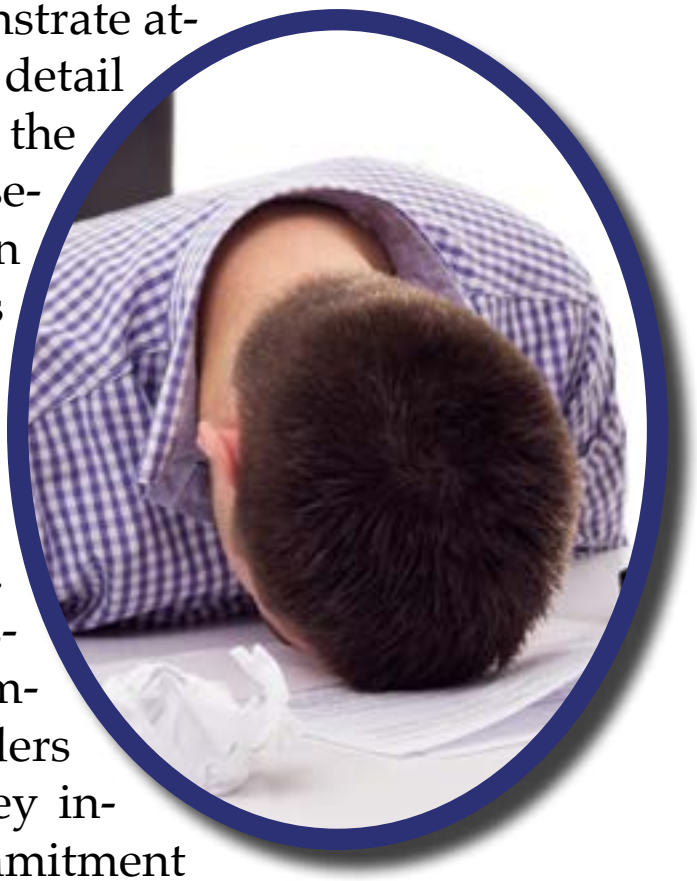
Hire a white-collar criminal defense attorney:

Entrepreneurs may have transactional and business lawyers to help them draft contracts. Yet as the business grows, leaders should also think about risks in the marketplace. They cannot live like an ostrich.

What does an ostrich do? Theory has it that an ostrich buries its head in the sand while in the presence of lions and hyenas; foolishly, the ostrich believes that if it cannot see the predator, the predator will not be able to devour the bird because the predator won't see it either. That strategy doesn't work out so well for the ostrich. And, it won't work out so well for business owners or executives that try to ignore the threat of big government.

The best offense is a great defense, so invest in writing out the corporate story. Create messaging that details every aspect of the corporate strategy.

Document everything from how the company processes incoming mail, to how the company attracts customers, to how the company sanitizes the bathroom, to how the company deals with complaints. The writing may seem tedious. Yet a written plan will demonstrate attention to detail, the kind of detail that lets investigators know the company takes compliance seriously. A compliance plan should protect the business and all team members.



To the extent possible, hire an attorney that specializes in white-collar crime. Task the attorney with assessing pertinent parts of the compliance manual. Business leaders protect themselves when they invest resources to show a commitment to comply with laws and regulations. Such an investment may open opportunities for leniency, deferred-prosecution agreements, or non-prosecution agreements in the unfortunate event that a government investigation begins.

The best chance to negotiate for leniency is before investigators bring charges. If a business gets appropriate counsel, leaders may minimize disruptions that could obliterate the business, and lead team members to prison.

Conduct an Internal Investigation:

Despite best efforts, and a strong compliance program, businesses sometimes learn of wrongdoing within the organization. If that happens, the business should take immediate, pre-emptive action. One proven technique that has saved many businesses and business leaders from prosecution stems from internal investigations.

If a business leader conducts regular compliance training and auditing, those efforts could potentially lead to the discovery of wrongdoing. At that stage, the business executive must make a decision on how to proceed. As an example, we can cite the case of Robert Smith, Chairman and CEO of a private equity group.

He formed the Excelsior Trust in Belize and Flash Holdings in Nevis. Smith relied upon third parties to conceal his beneficial ownership and control of those companies, but he controlled both offshore structures; Smith used those entities to avoid paying U.S. taxes.

To facilitate the venture, he relied upon foreign bank accounts in the British Virgin Islands and Switzerland to hide

assets from the IRS and from the U.S. Treasury Department. As a result of his financial structuring, Smith did not report more than $200 million in partnership income.

Authorities did not know about Smith's criminal behavior. Yet, Smith understood that he broke laws. When pressured by a Swiss Bank to self-report, he was slow to come to the table. He continued to file false documents.

At some point, he began listening to a lawyer that persuaded him to cooperate and work toward a non-prosecution agreement with the Department of Justice. Smith had to forfeit claims of more than $300 million. Had he waited for the government to bring an indictment, he would have also had to litigate his way out of criminal charges that could have led to multiple decades in federal prison.

For more details, take a look at the following press release and accompanying documents:

» Press Release: Private Equity CEO Enters into Non-prosecution Agreement on International Tax Fraud Scheme and Agrees to Pay $139 Million, to Abandon $182 Million in Charitable Contribution Deductions, and to Cooperate with Government Investigations

  ◊ https://www.justice.gov/opa/pr/private-equity-ceo-enters-non-prosecution-agreement-international-tax-fraud-scheme-and-agrees

» Statement of Facts: Exhibit to Robert E. Smith Non-Prosecution Agreement

◊ https://www.justice.gov/opa/press-release/file/1327911/download

» Non-Prosecution Agreement

◊ https://www.justice.gov/opa/press-release/file/1327906/download

How did Smith persuade the government to issue a non-prosecution agreement? Well, from the documents above, it becomes clear that he served up a bigger fish. As a result of Smith's cooperation, the government brought criminal charges against the CEO of a computer company.

Government investigators will always look for a bigger fish. That strategy feeds the ecosystem of mass incarceration. When our government creates incentives to bring more people into the system, everyone becomes vulnerable. For that reason, it's best to develop a best-practice compliance system, with total awareness that "Big Brother" is always watching, as George Orwell advised.

Review Your Insurance Policy:

Many corporate insurance policies include fraud-protection provisions. Those policies may cover both legal costs

and fines (up to a predetermined dollar amount). An effective policy protects officers and directors from the enormous litigation costs that accompany a government investigation. We encourage business owners to understand the costs of litigation, and to purchase an appropriate amount of insurance.

Effective business leaders should develop a solid appreciation for the financial costs associated with defending against a government investigation. Consider, for a moment, the process:

» Investigators will subpoena corporate documents.

» They will review every email, invoice, sales script, advertisement, receipt, contract, and so forth.

» They will take notes as they question witnesses.

That investigation will result in tens of thousands of pages, potentially millions of pages. It may also include hundreds of hours of recorded phone calls.

Business leaders should have a realistic understanding of the evidence that investigators will accumulate. On the government's side, dozens of agents and interns will sift

through the evidence, categorizing it in a well-organized manner.

They do not have to be sensitive to costs, unlike the target of the investigation. Investigators can deploy enormous resources, without consideration of a cost-benefit analysis. The investigators then deliver all of that information to government attorneys. Those attorneys will use that evidence to bring charges against individuals and potentially, the business.

Discovery:

When people hire defense attorneys to represent them in a government investigation, those defense attorneys look forward to the "discovery" phase. While the business owner will consider the mountain of evidence a burdensome nuisance, the defense attorney may see something else: billable hours.

Indeed, the defense team will insist upon reviewing every piece of evidence the investigators accumulated. They will insist on listening to every recording, watching every video, reading every note that memorialized what a witness revealed. Attorneys review the evidence to prepare for the case, to protect the client, and to make sure that they're ready to defend against accusations. Without insurance, the client ends up paying for those hours, at great expense.

In big cities like New York, San Francisco, Chicago, or Washington DC, defense attorneys that specialize in government investigations bill at rates that may shock the conscience of a typical business owner. Why? Because those attorneys are in the business of *practicing law*. In other words, attorneys need to stay current with case law and regulations and defense strategies.

To be the best in the world at what they do, attorneys must invest countless hours researching decisions without pay. Clients therefore pay for that expertise at rates that may exceed $2,000 per hour.

Multiply that number by the hundreds (or thousands) of hours necessary to read the mountains of evidence that investigators present. For this reason, legal costs associated with defending against a government investigation can easily surpass $10 million for some businesses.

Such fees can decimate a company that does not have adequate insurance. For individuals that lack insurance indemnifying them against legal fees, a government investigation can bring enormous personal stress and lead to personal bankruptcy.

Consider the case of Rod Kazazi, who held the position of Chief Operating Officer for a real estate development company when the Federal Trade Commission sued his company for violating the Federal Trade Commission Telemarketing Sales Rule and the FTC Act.

Rod hired former Assistant U.S. Attorney, David Wiechert, to represent him in the matter. Since Rod lacked financial resources to litigate the case, the attorney persuaded Rod to cooperate with the investigation. His cooperation could potentially shield him from liability on a judgment that would exceed $100 million.

In order to settle the case, Rod Kazazi agreed to provide false and unsubstantiated testimony to support the Federal Trade Commission's case. He also agreed to make a payment of more than $250,000.

In crafting the settlement agreement, the FTC attorneys slipped in misleading language that would protect them, at the expense of Kazazi's attorney. Kazazi's attorney did not catch one particular sentence in a settlement agreement spanning several thousand words.

As a result, the FTC later filed documents to void Kazazi's settlement agreement, and also hold the attorney personally liable for more than $250,000.

Key Takeaway:

» Business leaders should get a full understanding of the costs associated with defending against a government investigation. With that understood, each business leader should consider purchasing an insurance policy to cover the potential costs of litigation as soon as is practical.

Organize Records:

Business leaders invest well when they build effective and well-organized record-keeping systems. In the startup phase of a business, the organizational structure may exist in the founder's head.

All too often that structure remains with the founder, even though the company would benefit by documenting the corporate policies and procedures. By investing to build exceptional record-keeping systems, an company simultaneously invests in risk management against government investigations.

As the company grows, leaders of business should take time to document strategies and procedures. To the extent that they tell the company's story well, they build a protective mechanism. Clear records will help them run the company better, and also minimize disruptions in the event of litigation—assuming there's a solid commitment to building an honest and ethical organization.

When the company has sufficient resources, the best step would be to build an effective Customer Relationship Management (CRM) system. Some examples of CRM companies include Salesforce, Zoho, and Pipedrive. Those companies charge a per-user fee that may range from $30 a month to more than $200 a month, per seat. Great companies use CRMs for many reasons, including:

- Tracking their relationships with every consumer,
- Measuring return-on-investment with regard to marketing, sales, and operations,
- Making certain that all team members relay the right corporate message to consumers, and
- Creating a central repository for all corporate communications, records, and transactions.

An investment in a CRM can protect against government investigations. It can also help the business track the customer journey and more effectively communicate the company's value proposition to consumers.

A CRM becomes especially effective for business leaders that invest the time and energy to document their company's workflows. Regardless of whether the company invests in a CRM, the company should definitely invest in a system to organize and secure files—especially when it comes to storing data on customers. A data breach of customer information can lead to civil investigations with severe penalties—especially if the company is later determined to have acted recklessly with consumer information.

Remember that the destruction of company records during a government investigation can lead to criminal charges for obstruction of justice, or other crimes. The more leadership teams understand how much time, energy, and

resources that government investigators will invest to build a case, the more they appreciate the need for caution.

Under the ostensible guise of furthering their agency's mission, unethical government attorneys may suborn perjury or hide evidence that could prove favorable to an individual or business they want to target. Good leaders will invest in transparency, knowing that at any time, government investigators may be listening or monitoring a business's activities.

Talking with Government Investigators:

The Fifth Amendment of the U.S. Constitution protects people from having to speak with a government investigator. No one can be compelled to provide evidence that could, theoretically, be used against a person. All Americans should understand that government investigators go through extensive training to pull evidence they can later use against a person.

If a government investigator asks questions, remember that the investigator is trying to gather evidence to build a case. The investigator may say that he is simply trying to get an understanding of what happened. Getting to the truth, however, doesn't advance the investigator's career. Investigators get promotions when they build cases against people and businesses that lead to findings of liability or guilt.

With that in mind, remember that no one has to talk to a government investigator. But if a person chooses to speak with a government investigator, that person should follow two principles:

Principle 1:

» If a person chooses to speak with a government investigator, the person should not lie. Lying to a government official is a federal crime, punishable by up to five years in federal prison—for each lie.

Principle 2:

» If a person chooses to speak with a government investigator, the person should hire competent counsel. Although the lawyer cannot protect a person from lying, the lawyer can better advise the person on how government investigators may use any statements to build a case to reach the investigator's agenda. Make no mistake, the investigator aspires to bring charges against people or businesses.

Just as some business leaders will do or say anything to increase profitability, some government investigators will do or say anything to induce people to incriminate themselves or others. They want evidence that lead to findings of liability, or guilt.

Compliance Training

Lesson Six

Good employees begin their careers with good intentions. They want to do their job, earn a living, and pursue future career advancement. Unexpected circumstances may change a person's behavior. A robust compliance program can alter the equation.

Proper training builds a two-tiered system that both reduces a company's exposure to charges of fraud and its risk of becoming a victim of the fraud itself. It creates a supportive corporate culture that can remediate fraud before it occurs.

Effective compliance programs may keep top-of-mind the consequences of violating rules, regulations, and laws. People may be less inclined to engage in misbehavior when they understand the costs and penalties associated with a government investigation or prosecution for white-collar crime.

Good compliance programs can make all the difference. The more proactive measures a company takes, the more effectively it can show a good-faith effort to comply with laws and regulations. Good compliance lessens the the possibility of litigation.

Establishing a compliance and training system begins with a commitment to transparency. The first step would be to document the company's story and the value proposition it offers to consumers. The next step would be to write a process map and training schedule. The more detail leaders can bring to the process map, the more they will minimize exposure or vulnerability to a government investigation.

Ideally, the process map would include details of every function, including:

- How the business goes about recruiting staff,
- How the business organizes its hierarchy of positions,
- How the business compensates staff members,
- The roles and responsibilities of each staff position,
- How the company trains staff members,
- How the company attracts customers,
- How the company selects vendors,
- How the company processes customer orders, and
- How the company retains records.

Documenting the company story should show the company's good-faith effort to operate in compliance with all regulations and laws.

Further, the training should help all stakeholders understand consequences that can follow for those who fail to comply with the company's policies and procedures. Resources from the Department of Justice and various regulatory agencies show that transparency goes a long way toward protecting the business and the people that build careers in the business.

Training will lessen a business's exposure to charges of fraud, but it can also lessen a company's risk of becoming a victim of fraud. Our team members at Compliance Mitigation have worked with more than 1,000 people that have been charged with white-collar crimes.

Those people claim to have begun careers with the best of intentions. Somehow, circumstances changed for them. As a result, some of them became less vigilant about ethics or morality. Other times, they broke laws without knowing how they were putting themselves and their companies at risk. Good training will lower the company's risk profile. If that training includes lessons on the consequences of white-collar crime, more people may refrain from making the kinds of decisions that lead to criminal prosecution.

Overall Objectives:

1. If done well, compliance training will help everyone in the company get a clear understanding of corporate messaging. With better messaging, everyone on the

team should work together to build a more efficient and profitable enterprise.

2. The compliance training should help employees grasp internal rules and regulations critical to their job responsibilities and tasks.

3. A good compliance training program helps a company avoid penalties and even potential lawsuits.

4. Simultaneously, it should improve employee efficiency, productivity, and satisfaction on the job.

General Requirements:

For a compliance training system to work effectively, the leadership team must commit. If the leaders embrace the organization's goals and culture, the entire team will be more effective. Leaders should understand the relevant laws and know how to manage risk. Further, they should understand how lowering risk levels can lead to a company's positive reputation, lessening the potential for penalties or lawsuits.

Without good leadership, the company may be vulnerable. The regulatory landscape may change, which could bring further problems. Leaders should give clear guidance with regard to all compliance matters.

Besides commitment, the leadership team must implement the training effectively. Our team recommends creating logs to measure the following key objectives of compliance training:

1. Do all staff members understand their compliance responsibilities?
2. Does everyone understand how the compliance program reduces risk?
3. In what ways does the compliance program minimize potential legal liability?
4. How does the compliance program protect the company's reputation?
5. In what ways does the compliance program encourage integrity in the corporate culture?

Compliance training should cover internal regulations as well as external laws. Good leaders will understand the importance of identifying areas at high risk for non-compliance. They would then prioritize resources to document a strategy showing sensible controls. A good compliance system is like a good defense, providing leaders with confidence that they could respond to an investigator's questions.

After covering the high-risk areas, leaders should create systems to show their commitment to good corporate citizenship. For example, the company may develop policies to show the business's position on:

» Customer service standards,

» Anti-harassment,

» Anti-discrimination,

» Anti-sexual harassment,

» Conflicts of interest,

» Code of ethical conduct,

» Client confidentiality,

» Health and safety issues,

» Reporting protocols, and

» Issues particular to the business's industry.

We encourage leaders to bring the training to life with human stories and interactive exercises. The business may build a stronger case of showing its commitment to compliance by designing quizzes that measure what each participant learned. By making those participant responses a part of each employee's file, the company can build a stronger case of its commitment to compliance.

When employees earn their livelihoods from contacting clients over the phone, for example, leaders may want to include training exercises that profile dangers associated with the FTC's Telemarketing Sales Rule and the Do Not Call List.

The FTC regularly brings cases against small, medium, and large organizations if their investigations reveal a violation of FTC rules. The FTC's website highlights how those investigations have led to injunctions, fines, asset freezes, and massive judgments against business leaders that profess ignorance of how they were violating rules, regulations, or laws.

Consider the FTC case against Sanctuary Belize. In that case, a real estate developer used television commercials to advertise a 14,000-acre community in Belize. The commercials attracted viewers with images of crystal-clear water, palm trees, and white-sandy beaches.

Those commercials induced people to visit the company's website. The website brought attention to what the developer called "a world-class marina" and other amenities at the project. Consumers that wanted to learn more would

fill out a lead-capture form on the website, expressing interest in speaking with one of the developer's sales reps.

Telemarketers would contact the prospective buyers to schedule appointments. They would show a computer screenshare of the property and respond to questions from the consumers. If the consumer expressed interest, the telemarketer would coordinate a tour of the property in Belize. When consumers saw the property in Belize, they would make a decision on whether to purchase property in the development.

Using that technique, the developer entered into contracts with consumers, selling more than 1,000 homesites in his massive development. Sales surpassed $100 million.

The Federal Trade Commission launched an investigation, conducting an undercover call with the developer. Investigators at the FTC went through the entire telemarketing pitch. Although they never visited the property in Belize, they built a case to accuse the developer of deceiving consumers. The FTC alleged that developer deceived consumers with coordinated misrepresentations.

As a result of those charges, investigators from FTC stormed the developer's offices in Irvine, California. They seized computer records, all scripts, and other evidence to build a case. They began an investigation that turned telemarketers, managers, and leaders into either witnesses, subjects, or targets of their investigation. A lawsuit in fed-

eral court resulted in an asset freeze. Litigation expenses soared to several million dollars. In the end, a federal court issued a judgment in excess of $100 million. Further, the court placed enormous sanctions on the defendants, placing an earning cap of $5,000 per month on certain defendants; that earning cap would last a lifetime, or until the FTC fully recovered the full $100+ million judgment.

Had the company made a bigger investment in documenting the story, as well as its commitment to compliance training, the company's leaders may have had a better defense against FTC allegations that they were operating a scam.

Regular Training:

Regular training represents another key component to an effective compliance program. If the program does not offer regular training, it will not move the needle in arguing for leniency or non-prosecution agreements in a government investigation. The company must show a true commitment to building a culture of truth, honesty, and transparency.

A good online system that makes all of the training material easily accessible would show such a commitment to compliance. Some training programs may require interactive exercises, while others may require independent learning. All compliance programs should have a takeaway,

showing that participants are learning. When companies build records of compliance training, they protect the enterprise, the leaders, and the entire team.

Each component of the compliance training program should include a designated person, or responsible party. That person should have the appropriate training to oversee compliance. For example, the person in charge of training telemarketers should show fluency with the FTC Act and the Do Not Call List.They should be able to show how and why the company trains all team members to comply with such rules.

It's important to ensure that all employees have an opportunity to speak with a responsible party. The company must be able to tell a story demonstrating the investment it made to operate in accordance with all regulations and laws.

Regular Analysis:

With changes in the regulatory landscape, an enterprise must show a concerted effort to stay on top of changes in laws and regulations and a pattern of continuously analyzing the effectiveness of its compliance or training program. Leaders should record every change, showing the company's commitment to excellence. By documenting best practices, the company goes a long way toward building credibility with investigators.

Some useful tools to demonstrate a willingness to analyze and improve may include:

- Confidential performance reviews from immediate superiors,
- Confidential performance reviews from subordinates,
- Randomized peer reviews,
- Quarterly reviews by senior management,
- Periodic company-wide town halls to discuss the general direction of the company and important corporate developments,
- Management accessibility via internal email, and
- Documented strategies for internal corporate communications.

An effective compliance program will show a company's commitment to do the right thing all the time, leading to more confidence that the enterprise can withstand an inquiry by investigators.

Regulators look favorably upon such programs. By enacting steps to analyze and improve compliance policies, leaders show that they are not running the company by the seat-of-their pants, and that they're not engaging in willful blindness that can lead to charges of criminal negligence.

Case Study:

Members of our team at Compliance Mitigation served time alongside thousands of other people who were convicted of white-collar crimes. We knew one person who owned a brokerage firm that specialized in trading bonds. As the company grew, the owner began to delegate responsibilities for day-to-day trading activities.

Instead of overseeing trades, the owner focused on bringing in more capital. That strategy would have been fine, provided that the owner created well-documented and vetted compliance systems. Sadly, the owner did not.

Changing market conditions resulted in one of the lead traders making a series of unprofitable transactions. The trader then launched a series of events to cover up his decisions. When markets went against him, he lost more money than authorized, resulting in a margin call. The owner said that he was not aware of the losses, and he lacked the capital to meet the margin call. Chaos ensued, leading to a flash crash and obliterating the company's entire portfolio.

The owner of the bond trading firm lost everything. A government investigation followed. Prosecutors brought charges against many people, including the owner for his criminal negligence in failing to supervise employees. After a guilty verdict, a judge sentenced the owner to serve a prison term of longer than 10 years and saddled him with

a restitution order measured in the hundreds of millions of dollars.

Our team at Compliance Mitigation cannot vouch for the validity of what the owner told us—after all, we met him inside of a federal prison. On the other hand, we can say that if he had devised a better compliance system, he would have had a stronger defense against the charges that the government brought against him.

Effective Compliance Programs:

Like a three-legged stool, in order to stand, an effective compliance program should have three components:

1. The program should be clear with its objectives, communicating a commitment to compliance for all members of the enterprise;

2. It should show a commitment to transparency; and

3. It should include training on well-documented written policies, procedures, and standards of conduct. Having clear written policies and procedures in place that describe compliance expectations fosters uniformity within the company.

Without all three components, the compliance program will not serve much purpose in protecting the leaders or members of the enterprise. A clear authority figure should

oversee the compliance program, and the person in that role should have appropriate training for oversight. That person must accept responsibility for staff training and demonstrate a good-faith effort to ensure every person in the enterprise understands the purpose behind every policy. Some compliance training will be basic, essential for all new hires. Other training modules may require monthly or even daily accountability logs.

A good system will encourage two-way communication throughout the organization. All team members should express confidence that the organization will consider their ideas for improvement. If the organization is willing to listen to concerns, the company can strengthen its defense of its commitment to act as a good corporate citizen.

All compliance training should include steps to document how the responsible person within the company monitors and audits compliance. A robust monitoring and auditing system may induce all company representatives to comply and shows corporate commitment to doing the right thing. Such tactics should:

» Lessen the company's exposure to risks,

» Contribute to more efficient operations,

» Improve corporate messaging,

» Heighten each team member's awareness of the dangers of government investigations, and

» Offer more insight to the risk levels associated with white-collar crime.

Corporate leadership must have the courage to be swift and certain when it comes to discipline. Sometimes, such a commitment can lead to an ethical dilemma. If a person serves in a leadership role and has a history of being a rainmaker for the company, owners may be reluctant to discipline the individual for noncompliance. Yet if the rainmaker undermines the enterprise's commitment to compliance, the level of risk increases, often well in excess of the perceived benefit of the business generated by such rainmaker.

Again, leaders protect a company with well-documented commitments to transparency. If a team member fails to comply with program requirements, a clear record should show the appropriate corporate response.

When a company identifies vulnerabilities or violations through monitoring and auditing, management must take timely, consistent action to correct the issue. No company can implement a compliance program expecting to have considered all possibilities. We never know what we don't know. For this reason, leaders within the enterprise should build a record of analyzing corporate compliance and making improvements when necessary.

Defining a Company's Compliance Program:

Google caught the world's attention with its simple corporate motto: "Don't do evil." Since then, it's become the target of several government investigations.

A company strengthens itself when it clarifies the corporate mission, then builds a compliance program that reflects a commitment to the mission. To that end, a company should establish and maintain a culture that promotes:

- Quality and efficiency,
- High standards of ethical and business conduct,
- The effective operation of the business,
- High-standard maintenance of customer, client and vendor relationships, and
- The prevention, detection and resolution of conduct that does not conform to the company's standards and policies and applicable law.

A commitment to compliance should reflect those qualities above. It should apply to all company personnel equally, including but not limited to senior management, administration, personnel, ongoing contractors and all full-time and part-time employees of an organization.

All company programs should include elements that reflect best practices, including:

1. Written standards, policies and procedures to promote the company's commitment to compliance with its own proscribed code of corporate conduct, applicable laws and regulations,

2. Designation of an employee as the Compliance Officer (at least, as a part of the employee's overall job description) or the hiring of a full-time Compliance Officer charged, with the responsibility of implementing and monitoring the Compliance Program,

3. Designation of a Compliance Committee, if the corporate size warrants,

4. Regular, effective education and training programs for all personnel as appropriate to their functions,

5. A process to receive complaints concerning possible Compliance Program violations, procedures to protect the anonymity of complainants to the extent possible, and policies that protect complainants from retaliation,

6. Granting the Compliance Officer and/or the Compliance Committee, as the case may be, sufficient authority to investigate, report and make recommendations directly to senior management and the Board of Directors regarding any irregularities and all findings,

7. A process to respond to allegations of improper activities and the enforcement of appropriate disciplinary

action against personnel who have violated policies, laws, regulations, or program requirements,

8. Periodic audits or other methods to monitor compliance and assist in the reduction of problems in any identified areas,

9. A process for investigating and resolving any identified problems, after investigation, report and recommendation by the Compliance Officer and/or Compliance Committee, as the case may be, and

10. A document stating the foregoing points that all stakeholders sign, including a member of senior management, the Compliance Officer and the employee, either upon initial implementation of the program or upon the hiring of any new employee.

The company's compliance program should grow stronger and more effective over time, becoming an integral part of the corporate culture. When company leaders fail to implement a compliance or training program, they expose themselves and their team members to higher levels of risk.

As stated at the start of this module, the company should create an accurate organizational chart, defining excellence within each role of the organization. Such an organizational chart should become a part of the enterprise process map, illustrating the functions and responsibilities of every role.

For example, the organizational chart should articulate the role of senior executives, showing responsibility for:

1. Evaluating risks that result from non-compliance with rules and regulations,
2. Approving and supporting the compliance program, and
3. Overseeing the performance of the compliance program to reduce risk.

Show who bears responsibility to train on:

1. Compliance with laws and regulations,
2. Regulatory requirements of each functionary within the organization,
3. The company's internal rules and codes of conduct, and
4. How the company works to remediate weaknesses and prevent violations.

Compliance Officer and responsibility for:

1. Coordinating audits and examinations in connections with laws, regulations and corporate rules and codes of conduct,
2. Acting in an advisory capacity on the company's policies and procedures,

3. Monitoring corporate transactions, functions, events and internal systems seeking violations and to uphold the integrity of the organization, and

4. Communicating issues to Senior Management and the Board of Directors.

Employees acknowledge responsibility for:

1. Acknowledging that they've been trained in the compliance program,

2. Acting in accordance with the company's compliance program,

3. Partaking and engaging in all of the company's compliance program activities,

4. Reporting any violations of the company's compliance program to either a direct manager or the Compliance Officer/Committee, confidentially or otherwise, as the case may be.

As a living, breathing entity, the enterprise should maintain the compliance program to protect against disruptions from litigation and government investigations, as well as to show a commitment to professionalizing the business. An effective program would demonstrate how the company pursues excellence, which leads to more success for all team members.

Internal Fraud

Lesson Seven

Internal fraud begins with a person's intentional actions. At Compliance Mitigation, we help business leaders avoid complacency and open their eyes to signs of internal fraud that could expose the business to investigations.

Confucius said, "By three methods we may learn wisdom:

- *First by reflection, which is noblest;*
- *second by imitation, which is easiest; and*
- *third by experience, which is bitterest."*

By reflecting upon the actions of others and focusing on potential hazards, we prepare a company for long-term success. We use examples that follow for people who went through investigations and prosecutions to prompt better critical-thinking skills.

The more people know, the more we encourage them to act in compliance with rules and regulations. Members of our team learned through costly, bitter experiences. By sharing those experiences with others, we help team members make better decisions, and lessen a company's exposure to risk.

Although we can control our own behavior, we don't always have an ability to know how others will behave. When business leaders delegate responsibilities, they simultaneously raise their level of risk. Business leaders may not know what a team member is saying to a customer or how that team member may be acting in fulfilling job responsibilities. When that happens, the team member may expose the entire company to interference from regulators, or losses from internal fraud.

For example, consider Justin, a co-founder of one of our companies.

Justin graduated from USC and went on to become a stockbroker. While employed as a stockbroker at UBS, he executed market trades on behalf of people that managed private hedge funds. In that role, Justin had insight into account balances for the clients he served; he could also review balances in each of the client accounts at the hedge-fund. UBS trusted Justin took to look after the interests of his clients, and also after the interests of the firm.

When Justin walked into a meeting with one of his clients, he also met with people who had invested in the hedge fund. Those investors showed Justin an account statement that they had received from the hedge-fund manager. When Justin saw the statement, he knew at once that the document had been fraudulently inflated. His client had manipulated the statement to show balances that the client wanted to see, rather than what the account held.

Justin had been earning enormous commissions from the account. Despite seeing first-hand evidence of the fraud, he chose to remain quiet so as not to disturb the income stream from commissions. Rather than reporting the fraud, Justin allowed his client to continue deceiving investors. As a result, Justin immersed himself into an internal fraud that cost his employer millions of dollars. When authorities discovered the fraud, Justin lost his job.

Justin had deceived himself into believing that since he wasn't the person manipulating the financial statements, he wasn't responsible. Yet by continuing to claim commissions for trades that he knew had been predicated on fraud, he became complicitous.

Fraud charges may stem from direct participation, or even from the observation of others that participate in fraud. As a result of his complicity, prosecutors brought criminal charges against him. While in prison, he said that while he was in the midst of the crime, he didn't realize the extent of his wrongdoing.

Business leaders and team members can learn from such examples. Many people do not set out to participate in fraudulent schemes. They fall into situations on the job or go through complications in life. Those situations can lead to a dilemma; doing the right thing can have bad consequences:

» A person can lose an income stream,

» A person can be ostracized on the job, and

» A person may have to serve as a witness against someone he or she cares about.

We'd like to believe that people of good character always act appropriately. Yet with the growing number of guilty pleas for white-collar crimes like fraud, bribery, or other types of self-dealing acts, people's characters are constantly tested.

Our team at Compliance Mitigation believes that business leaders would, therefore, be wise to invest more time and resources in training. Despite good intentions, opportunities or bad actors can tempt people. And people can delude themselves with all types of lies to excuse their behavior. When they do, they put their liberty on the line, and they expose the company to enormous costs.

Business leaders that invest time to train may lower a company's risk profile and a company's vulnerability to internal fraud. In earlier modules, we've noted three components that may increase possibilities for fraud:

1. Financial Pressure - such as significant personal debt, credit problems, or some kind of emergency.

2. Opportunity – the ability and capability to take advantage of an opening in either your security system or system of checks and balances.

3. Rationalization – justifications for illicit actions.

Since most people don't seek employment with an intention to commit fraud, it's difficult to predict a person's character during the hiring process. The thought of committing fraud usually occurs over time as circumstances and/or disillusionment sinks in. For this reason, compliance programs should task a specific individual with responsibility to conduct spot checks, or audits, with an expressed goal of looking for signs of internal fraud.

Without good compliance, internal fraud may go undetected for years, as in the following examples:

Lifestyle doesn't coincide with income levels

» Rita served as the Comptroller of a small city in Illinois. The $80,000 salary she earned would not support her luxurious lifestyle, including a $2 million custom RV, a vacation home, and a world-class horse breeding farm with 400 horses. Despite splurging on so many extravagant purchases, her peers did not suspect wrongdoing. Over the course of two decades, Rita's internal fraud led to the embezzlement of more than $53 million, a huge sum for such a small city. By abusing her position of trust and authority, she schemed to funnel

public money into her private accounts. While Rita was on leave, a temporary worker found confusing paperwork. When the temporary worker called the city's bank, they discovered the fraud. A federal judge sentenced Rita to serve more than 19 years in prison.

Personal financial difficulties

» Barbara, a long-time secretary and clerk at a local church, found herself in a bind. She struggled with a gambling addiction that sent her into a spiraling debt. Over nine years, Barbara's losses exceeded $800,000. To cope, she pilfered money from the church's collection basket. After authorities uncovered her fraud, they charged her with crimes. A conviction led to Barbara's nine-year prison term. She claimed that she didn't know her actions could lead to imprisonment. Such statements give us reason to suggest that compliance programs should include human stories of people that broke the law; they should highlight the fallout for business owners and the person who broke the law.

Lack of Transparency

» Brian, a charismatic physician, served as the administrative director for 20 years in his practice that included 12 physicians. Despite a robust practice, the group showed paltry profits. Brian had a strong personality, and he could bully the other partners into believing that expenses were high—without providing documenta-

tion. If people questioned him, he had the power to ostracize them, or provide less desirable working conditions. Finally, one of the partners hired an outside firm to investigate. The internal investigation showed that, over two decades, Brian bilked the practice out of more than $25 million. A conviction led to a prison term of more than 20 years.

An employee colludes with vendors

» Tony, a construction manager for a fast-growing media company oversaw projects around the world. In that role, He had the discretion to assign contracts to various suppliers, contractors, and subcontractors. Some of those contracts exceeded millions of dollars in value. Although his employer paid Tony an excellent salary, he supplemented his income by accepting bribes from contractors that wanted to do business with him. The people paying the bribe would get the job, but without having to compete on price, victimizing Tony's employer. Over the course of five years, authorities accused Tony of participating in a bribery scheme that exceeded $5 million in value. After a guilty plea, a federal judge sentenced Tony to serve a five-year prison term. Further, besides suffering losses as a result of Tony's betrayal, the company lost millions of dollars in additional legal costs resulting from both an internal investigation, and a government investigation.

Minimizing Vulnerabilities:

Although we can control our own behavior, none of us can control the choices that other people make. A person may seem to be a pillar of propriety, but circumstances may lead that person to make bad decisions, or to act out of character. Those bad decisions can lead a business, or other people, into investigations that reveal internal fraud and potential liability to criminal charges.

To minimize vulnerabilities, we recommend that business leaders create compliance systems and best practices for their organizations. Good CRM systems may help. Companies that train others on the dangers of white-collar crime may go a long way toward minimizing vulnerabilities to internal fraud.

Minimize Vulnerabilities

Lesson Eight

Companies may remain "willfully blind" of what prosecutors expect to see in compliance programs. Yet blindness will not protect them.

Prosecutors want companies to show a good-faith effort to operate in compliance with laws and regulations. They should review the programs regularly and offer new material regularly. Failing to update compliance programs may result in a company being more vulnerable or make the company less likely for leniency.

Compliance requires constant updating and universal enforcement on a regular basis. Prosecutors want to see compliance as an inherent part of a company's corporate culture, inducing employees to act appropriately at all times. Good compliance programs should promote transparency and efficiency.

The Department of Justice has clearly designated corporate fraud as a hot button topic, but also provided guidance on how to best avoid being the subject of an investigation or prosecution.

For reasons expressed throughout these modules, every business leader should consider possible steps to lessen potential exposure to a government investigation. Three suggestions follow:

1. Show a commitment "to doing good" in all communications.

2. Document processes that show a commitment to operating the business with principled, transparent policies that are easily defensible.

3. Train all team members to understand the corporate culture, and also the reasons behind every policy in place.

These three components would go a long way toward protecting businesses and individuals.

Government Officials:

In 1991, the U.S. Sentencing Commission (USSC) amended its guidelines. The amendments incentivized business owners to act in compliance with regulations and the law. Those changes opened opportunities for prosecutors to grant leniency, non-prosecution agreements, or deferred-prosecution agreements to businesses that put "effective compliance programs" in place.

Theoretically, if business leaders designed effective compliance programs, their efforts would show a good-faith effort toward corporate responsibility. By building a record demonstrating that they want all team members to act appropriately, leaders reduce risk levels. Although no one can eliminate the possibility of a government investigation, good records will serve as an excellent defense mechanism.

As we've stated throughout, although business leaders can control personal decisions, they cannot observe decisions that other people on their team make. For those reasons, leaders should add training on the personal costs that can accompany an investigation or a prosecution for white-collar crime.

Agencies within the Department of Justice now incentivize businesses to make bigger investments in compliance. Guidance from 2019 advises federal prosecutors to consider the following questions when evaluating corporate compliance programs:

1. Is the program well designed?
2. Is the program being implemented effectively?
3. Does the compliance program work in practice?

In 2020, the DOJ emphasized another two key points with its publication of: Evaluation of Corporate Compliance Programs (2020 Guidance):

- https://www.justice.gov/criminal-fraud/page/file/937501/download

First:

Corporate compliance programs, to be deemed genuine and effective by the DOJ, must be examined, tested, and updated on a continual basis, including (and perhaps especially) during a government investigtion.

Compliance efforts should integrate current data analytics, capabilities wherever possible. If deficiencies are found, then changes should be made, and the 2020 Guidance makes clear that DOJ expects regular review of compliance efforts.

Second:

The quality of a company's compliance program continues to be a major factor in deciding on the appropriate resolution of a government investigation. The 2020 Guidance makes clear a program's effectiveness will be considered at the close of an investigation as well as when the underlying company conduct occurred.

Consequently, under DOJ policy, the strength of a company's past and present compliance efforts will ordinarily have an effect on the terms of a resolution, including the often quite important matter of whether a monitor is required (and the scope of a monitorship).

The DOJ's guidance can help business leaders make decisions to lessen exposure to investigations.

Effective compliance programs will not only show people what they should do, it will help those people understand what they should not do. In addition, they may also profile the consequences that follow for bad behavior.

If a company invests the time to show a person how to make the right decisions, and it requires the people to acknowledge that they understand corporate policy, the business protects itself. Good compliance programs will encourage both corporate accountability, and personal accountability. If there is a breach of policy, the company should create a record and demonstrate the steps that it has taken to make things right.

Two questions that investigators may ask include:

» Has the company ever terminated or otherwise disciplined anyone for the type of misconduct at issue?

» Have the disciplinary actions and incentives been fairly and consistently applied across the organization?

To demonstrate individual accountability, the company will record disciplinary measures taken against people charged with violations of compliance policies. If a company shows that it pays more than lip service to compliance, it may lessen exposure to a government investigation.

Compliance programs serve as an insurance policy. Although business leaders may strive to do the right thing every time, rogue employees can expose the business to risks. The compliance program may influence the lens through which prosecutors view the company. That said, some metrics show that the mere existence of a compliance program *doesn't show commitment* to compliance. Solely requiring employees to sign forms showing that they're familiar with the corporate polices won't move the needle if a pattern of fraud is uncovered.

In 2012, the prosecutors brought criminal charges against Garth Peterson, a trader at Morgan Stanley. Documents noted that Peterson had gone through seven compliance-training sessions and 35 related reminders on bribery. Despite that training, he pleaded guilty to bribery charges. Compliance initiatives had little influence on Peterson, because he viewed them as pro forma, something he needed to do in order to keep his job.

If a business doesn't create a compliance program with robust follow-through, it may be ineffective and dubious from the perspective a government investigator. Prosecutors will not give credit for compliance programs that fail to inspire appropriate conduct.

A company protects itself when it comes up with innovative ways to help people within the organization embrace the principles of compliance—but also understand the consequences for non-compliance.

Designing A Compliance Program:

Compliance is not a "one-size-fits-all" proposition. Leaders within a company should:

» Document the reasons behind the compliance training.

» Show the tools, tactics, and resources they've implemented to train.

» Create accountability logs to show people that have gone through the training, encouraging them to self-report what they've learned from the program.

If the program doesn't work, the leader should show what adjustments he or she has made.

Federal and state regulations, as well as industry standards, evolve constantly. For this reason, leaders should conduct regular assessments to minimize the risks associated with noncompliance.

Risk factors:

» What inherent risks exist in the company's market?

» What efforts does the company leadership make to stay aware of the market?

» In what ways does the company solicit third-party expertise?

Objectives:

» What purpose does each module within a compliance program serve?

» In what ways do members of the team understand the objectives of a corporate compliance program?

Departmental Responsibilities:

» In what ways does the company delegate responsibility for compliance programs?

» In what ways does the company measure excellence in delivering compliance training?

» How does the company record employee buy-in of the training?

» What do team members or stakeholders understand about reporting metrics?

Training:

» What level of commitment does the company make to training?

» What efforts does the company make to update the training?

» In what ways can employees independently participate in computer-based training?

» How does the company measure employee engagement?

Corresponding Policies:

Like every individual has a personality, every organization has an identity. Different businesses will need a compliance program that matches the business's identity. Some organizations may require a policy that scrutinizes new hires more than others. For example, a business that controls financial information for consumers may require crim-

inal-background checks on all new hires, while a company that specializes in landscaping may not.

A compliance program should show a commitment to transparency. All policies should harmonize with the behavior of officials at the highest level. In this era of cloud-based computing, leaders may make use of computer-based training, encouraging members of the team to review lessons remotely. If employees have feedback, mechanisms should exist for them to provide feedback in a manner that will not undermine their position—provided they offer the feedback in a good-faith effort to promote compliance.

Summary:

In summary, the best way to minimize vulnerabilities to government investigations is to create a good compliance program that is consistent with the corporate culture. Document every practice within the company. Show the reasons behind the ways that the company makes decisions. Train team members on how to work within the framework of the corporate culture. Leaders may want to review guidance from the Department of Justice, and question whether the compliance programs they've put in place measure up.

A good tactic may include bringing in a neutral third party who has that credentials to ask the questions that investigators will ask. Create a program that will allow lead-

ers of the organization to respond honestly, with their dignity intact. When making a decision on whether to bring charges against a company, government attorneys will ask:

1. Is the program well designed?

2. Is the program being implemented effectively?

3. Does the compliance program work in practice?

If a company leader can respond to those questions as quickly as he can answer the questions regarding corporate profitability, the leader will have done everything possible to minimize vulnerabilities to a government investigation.

In our era of big government, that doesn't mean a government investigation will not begin. It only means that a company is in as good a position as possible. No one can change past behavior. But we all can work toward minimizing risks in the future.

Fraud-Response Plan

Lesson Nine

A Fraud-Response Plan serves as an insurance policy against disaster. No one wants to encounter a disaster, but if difficulties come, insurance provides a level of comfort against the loss. Similarly, it's best to prepare long before a government investigation begins.

In the absence of a plan, people may not know how to respond if they're confronted with questions—or a raid—by government agents. By responding without intention, people may inadvertently expose themselves, their colleagues, and their company to further liability.

The best time to minimize complications from a government investigation is before the investigation begins. Yet with millions of regulations in existence, a company may face a problem at any time. Good preparation in advance may lessen liability. By anticipating aggressive behavior for investigators, team members can respond in ways to protect rights and get better outcomes.

Previous modules offered insights we believe leaders should consider when designing an effective compliance program and risk-management strategy for their organizations. The more leaders customize their compliance and best-practice programs, the better they safeguard against intrusive investigations that could threaten the business and its team members.

Regardless of what efforts team members make to protect a company, possibilities always exist for a breakdown, or for a rogue team member that could expose the organization to liability. For that reason, all companies should create a plan that would coordinate a team response in the event of an inquiry from regulators or law enforcement.

Lack of Planning:

In the absence of a structured response plan, team members may not know what to do if they learn that authority figures have taken an interest in the company or in a team member. Sometimes, leaders act rashly. People have gone to prison for their response to a government investigation, rather than for the underlying reasons behind the inquiry.

Consider the case of the famous celebrity, Martha Stewart. Many people are familiar with her brand, which sells household products. In 2001, however, a personal scandal over a stock sale completely disrupted her life. Her response to a government inquiry led to criminal charges.

According to the U.S. Securities and Exchange Commission, in late December 2001, her stockbroker at Merrill Lynch, Peter Baconovic, called her. Peter revealed that Sam Waksal, the CEO of ImClone Systems had placed an order to sell all of his shares in his company as a result of an adverse decision by the Food and Drug Administration. In response, Martha sold approximately 4,000 shares that she owned, avoiding losses of more than $45,000.

When government investigators began making inquiries, Martha did not have a good plan. The responses she gave to the government investigators resulted in criminal charges. The fees and costs associated with the disruption likely exceeded several million dollars.

Besides losing money for legal costs, Martha's response to the investigation led to a prison term, a shareholder derivative suit against Martha Stewart and other directors at her company, and five months in prison. With a felony conviction, Martha endured lifelong complications, including bans on travel to some countries.

Clearly, Martha Stewart did not have a principled plan that would guide her response to a government inquiry. Sadly, many people find themselves in the same predicament. Those who operate businesses without designing a response plan for government inquiries may leave them-

selves vulnerable to knee-jerk reactions that can exacerbate troubles.

A lack of a plan can lead to confusion during the first few hours, days and weeks of an inquiry. The unfolding drama can distract team members, as everyone may worry about personal liability. If people don't know what to do, they may make futile attempts at self-preservation, such as destroying incriminating evidence, or lying to government investigators. Either response would expose the individual, and potentially others, to criminal charges.

Risk Management:

A good response plan will ensure that all team members have guidelines to follow. Whether government regulators inquire about business operations or potential fraud, everyone should know what steps to take. To protect both the business and the team members, corporate leaders should articulate the appropriate protocol any time an investigator makes an inquiry.

» Does everyone in your organization know how to respond in the event that an investigator asks a question?

Leaders can easily get an answer to that question by creating a plan. Then, they should create a training exercise for all team members. The more transparency leaders bring to an investigation-response plan, the more they will strength-

en arguments that the organization has made a genuine effort to act in compliance with all regulations and laws.

» Point for business leaders to consider:

◊ Regulators and judges are increasingly asking not just whether a company has an anti-fraud, anti-money laundering, or corporate ethics policy in place. They are also asking how well such programs work and whether their quality and results make sense. They are asking, in other words, how good are they? This trend raises the stakes for those charged with governance.

An example of an effective "anti-fraud policy" may prove helpful to business leaders that want to create an organizational-specific plan. Our team at Compliance Mitigation offers the following as a template:

INTRODUCTION

» Our company (the "Company") has a commitment to high legal, ethical and moral standards. We expect all members of staff to share this commitment. The Board of Directors tries to ensure that a risk (and fraud) awareness culture exists in this organization. Fraud is an ever-present threat and hence must be a concern to all members of staff. Our Company views fraud as an extremely serious matter and is committed to the promo-

tion of an Anti-Fraud Culture throughout the organization.

» We created this document to provide direction and help to those who find themselves having to deal with suspected cases of theft, fraud or corruption. This document gives a framework for a response, advice and information on various aspects and implications of an investigation. It is not intended to provide direction on prevention of fraud.

» This Policy applies to any irregularity, or suspected irregularity, involving employees as well as consultants, vendors, contractors, customers and/or any other parties having a business relationship with the Company. Any investigative activity required will be conducted without regard to any person's relationship to this organization, position or length of service. All managers and supervisors have a duty to familiarize themselves with the types of improprieties that might be expected to occur within their areas of responsibility and to be alert for any indications of irregularity.

DEFINITIONS – WHAT IS FRAUD?

» We define Fraud as "dishonestly obtaining an advantage, avoiding an obligation or causing a loss to another party." The term "fraud" commonly includes activities

such as theft, corruption, conspiracy, embezzlement, deception, bribery and extortion. It may involve:

- ◊ manipulation, falsification or alteration of records or documents;
- ◊ suppression or omission of the effects of transactions from records or documents;
- ◊ recording of transactions without substance;
- ◊ misappropriation (theft) or willful destruction or loss of assets including cash; and
- ◊ deliberate misapplication of accounting or other regulations or policies.

» The criminal act is the attempt to deceive, and attempted fraud is therefore treated as seriously as accomplished fraud.

» Computer fraud arises where information technology equipment has been used to manipulate programs or data dishonestly (for example, by altering, substituting or destroying records, or creating spurious records), or where the use of an IT system was a material factor in the perpetration of fraud. Theft or fraudulent use of computer time and resources is included in this definition.

» Some illustrations of incidents which would be classified as fraud are contained in Appendix A to this Policy.

THE FRAUD RESPONSE PLAN

» The purpose of the Fraud Response Plan (the "Plan") is to ensure that effective and timely action is taken in the event of a fraud. The Plan aims to help minimize losses, reduce liability and increase the chances of a successful investigation.

» The Plan defines authority levels, responsibilities for action, and reporting lines in the event of a suspected fraud or irregularity. It acts as a checklist of actions and a guide to follow in the event of fraud being suspected. The Plan is designed to enable the Company to:

◊ prevent further loss;

◊ establish and secure evidence necessary for criminal, civil and/or disciplinary action;

◊ determine when to contact the police and establish lines of communication;

- ◊ assign responsibility for investigating the incident;
- ◊ minimize and recover losses;
- ◊ review the reasons for the incident, the measures taken to prevent a recurrence, and determine any action needed to strengthen future responses to fraud.

COMPANY RESPONSIBILITIES

» The company will undertake fraud investigations where there is suspected fraud and take the appropriate legal and/or disciplinary action in all cases where that would be justified. Whether there is fraud (proven or suspected), the Company should make any necessary changes to systems and procedures to prevent similar frauds from occurring in the future. The Company should establish systems for recording and subsequently monitoring all discovered cases of fraud (proven or suspected).

» Responsibility for exercising disciplinary actions rests with the Director of Human Resources **[or the Director of Compliance, for a company large enough to have independent compliance personnel]**, although this should be done in consultation with other Executives where appropriate.

MANAGING THE RISK

The Executives (CEO and CFO) of the Company are responsible for establishing and maintaining a sound system of internal controls that support the achievement of Company policies, aims and objectives. The system of internal controls is designed to respond to and manage the whole range of risks that the Company faces. Managing fraud risk will be seen in the context of the management of this wider range of risks.

- Overall responsibility for managing the risk of fraud has been delegated to front line managers and an internal auditor (whose duties are defined below). Their responsibilities include:
  - developing a fraud risk profile and undertaking a regular review of the fraud risks associated with each of the key organizational objectives in order to keep the profile current;
  - designing an effective control environment to prevent fraud from happening;
- establishing appropriate mechanisms for:
  - reporting fraud risk issues,
  - reporting significant incidents of fraud to the CFO and Human Resources **[or the Compliance Department]**.

» making sure that all staff are aware of the Company's attitude to fraud and know what their responsibilities are in relation to combating fraud;

» developing skill and experience competency frameworks;

» ensuring that appropriate anti-fraud training and development opportunities are available to appropriate staff in order to meet the defined competency;

» ensuring that vigorous and prompt investigations are carried out if fraud occurs or is suspected;

» taking appropriate disciplinary action against supervisors where supervisory failures have contributed to the commission of fraud;

» taking appropriate action to safeguard the recovery of assets;

» ensuring that appropriate action is taken to minimize the risk of similar frauds occurring in the future.

Line Managers Responsibilities:

» ensuring that an adequate system of internal controls exists within their areas of responsibility and that controls operate effectively;

» preventing and detecting fraud;

» assessing the types of risk involved in the operations for which they are responsible;

» regularly reviewing and testing the control systems for which they are responsible;

» ensuring that controls are being complied with and their systems continue to operate effectively;

» implementing new controls to reduce the risk of similar fraud occurring where frauds have taken place.

Internal Auditor Responsibilities:

» delivering an opinion to the CFO and Audit Committee on the adequacy of arrangements for managing the risk of fraud and ensuring that the Company promotes an anti-fraud culture;

» assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness of controls commensurate with the extent of the potential exposure/risk in the various segments of Company's operations;

» assisting management in conducting fraud investigations.

Staff Responsibilities:

» acting with propriety in the use of Company resources and the handling and use of Company funds whether they are involved with cash or payments systems, receipts or dealing with suppliers or customers.

» being conscious to the possibility that unusual events or transactions could be indicators of fraud;

» reporting details immediately through the appropriate channel, if they suspect that a fraud has been committed or see any suspicious acts or activities;

» co-operating fully with whoever is conducting internal checks, reviews or fraud investigations.

FRAUD DETECTION

» Line Managers should be alert to the possibility that unusual events or transactions could be symptoms of fraud or attempted fraud. Fraud may also be highlighted as a result of specific management checks or be brought to management's attention by a third party. Additionally, irregularities occasionally come to light in the course of audit reviews.

» The factors which gave rise to the suspicion should be determined and examined to clarify whether a genuine mistake has been made or an irregularity has oc-

curred. An irregularity may be defined as any incident or action which is not part of the normal operation of the system or the expected course of events.

» Preliminary examination may involve discreet enquiries with staff or the review of documents. It is important for staff to be clear that any irregularity of this type, however apparently innocent, will be analyzed.

ACTION FOLLOWING DETECTION

» When any member of staff suspects that a fraud has occurred, he/she should notify his/her Line Manager or Internal Auditor immediately. Speed is of the essence and this initial report can be verbal and must be followed up within 24 hours by a written report addressed to the Line Manager/Internal Auditor which should cover:

◊ The amount/value if established.

◊ The position regarding recovery.

◊ The period over which the irregularity occurred, if known.

◊ The date of discovery and how the suspected fraud was discovered.

- ◊ Whether the person responsible has been identified.
- ◊ Whether any collusion with others is suspected.
- ◊ Details of any actions taken to date.
- ◊ Any other information or comments which might be useful.

» Before completing the report above, line management may want to undertake an initial inquiry to ascertain the facts. This enquiry should be carried out as speedily as possible after suspicion has been aroused: **prompt action is essential**. The purpose of the initial enquiry is to confirm or negate, as far as possible, the suspicions that have arisen so that, if necessary, disciplinary action including further and more detailed investigation may be initiated. The Internal Auditor is available to offer advice on any specific course of action which may be necessary.

» As the gravity of each irregularity might be different, a reporting member of staff may wish to act in accordance with the *"Policy on Reporting and Investigating Allegations of Suspected Improper Activities."*

REPORTING WITHIN THE COMPANY

» On verbal notification of a possible fraud the Line Manager/Internal Auditor must immediately contact the CFO. He/She will inform and consult with the CEO (General Director) in cases where the loss is potentially significant or where the incident may lead to adverse publicity.

» The CFO will maintain a log of all reported suspicions, including those dismissed as minor or otherwise not investigated. The log will contain details of actions taken and conclusions reached and will be presented to the Audit Committee for inspection annually. Significant matters will be reported to the Board of Directors as soon as practical.

» Where a member of staff is to be interviewed or disciplined, the CFO and/or Internal Auditor will consult with, and take advice from, the Director of Human Resources **[or Director of Compliance]**. He will advise those involved in the investigation in matters of employment law, Company policy and other procedural matters (such as disciplinary or complaints procedures) as necessary.

INVESTIGATION / FURTHER ACTION

» If it appears that a criminal act has not taken place, an internal investigation will be undertaken to:

◊ determine the facts;

◊ consider what, if any, action should be taken against those involved;

◊ consider what may be done to recover any loss incurred; and

◊ identify any system weakness and look at how internal controls could be improved to prevent a recurrence.

After proper investigation, the Company will take legal and/or disciplinary action in all cases where leaders consider further action appropriate. There will be consistent handling of cases without regard to position or length of service of the perpetrator.

» Where an investigation involves a member of staff and it is determined that no criminal act has taken place, the CFO will liaise with the Director of Human Resources **[or Director of Compliance]** and appropriate Line Manager to determine which of the following has occurred and therefore whether, under the circumstances, disciplinary action is appropriate:

- ◊ gross misconduct (i.e. acting dishonestly but without criminal intent);
- ◊ negligence or error of judgment was seen to be exercised; or
- ◊ nothing untoward occurred and therefore there is no case to answer.

» Where, after having sought legal advice, the CFO judges it cost effective to do so, the Company will normally pursue civil action in order to recover any losses. The CFO will refer the case to the Company's legal advisers for action.

» Where initial investigations point to the likelihood of a criminal act having taken place, the Executives (CEO or CFO) will contact the police (or appropriate Federal agency, as the case may be) and the Company's legal advisers at once. The advice of the police will be followed in taking forward the investigation.

» The investigations described above will also consider whether there has been any failure of supervision. Where this has occurred, appropriate disciplinary action will be taken against those responsible for this failure.

RECOVERY OF LOSSES

» The recovery of losses should be a major objective of any fraud investigation. To this end, the quantification of losses is important. Repayment of losses should be sought in all cases. Where necessary, the Company will seek external advisors and legal advice on the most effective actions to secure recovery of losses.

MANAGERS' DUTY OF CARE

» Managers conducting initial enquiries must be conscious that internal disciplinary action and/or criminal prosecution may result. If such action is later taken, then under proper procedure the member of staff concerned has a right to representation and may have the right to remain silent. Utmost care is therefore required from the outset in conducting enquiries and interviews.

» In addition, in order to protect the Company from further loss and damage from destruction of evidence, it may be necessary to suspend the member of staff concerned immediately after the allegation has been made or following the submission of the Manager's initial verbal report. Specific advice should be sought from Human Resources **[Compliance]** before proceeding.

PROTECTION OF EVIDENCE

If the initial examination confirms the suspicion that a fraud has been perpetrated, then to prevent the loss of evidence which may subsequently prove essential for disciplinary action or prosecution, the person heading up the investigation ("Head of Investigation") should:

» take steps to ensure that all original evidence is secured as soon as possible;

◊ be able to account for the security of the evidence at all times after it has initially been secured, including keeping a record of its movement and signatures of all persons to whom the evidence has been transferred. For this purpose, all items of evidence should be individually numbered and descriptively labeled;

◊ not alter or amend the evidence in any way;

◊ keep a note of when investigators came into possession of the evidence. This will be useful later if proceedings take place;

◊ remember that all memoranda relating to the investigation must be disclosed to the defense in the event of formal proceedings against an employee, so it is important to carefully consider what information needs to be recorded. Particular care must be taken with phrases such as "discrepancy" and

"irregularity" when what is really meant is fraud or theft;

◊ ensure that electronic evidence is appropriately handled by certified specialists.

HEAD OF INVESTIGATION

» Executives of the Company will nominate in writing the Head of Investigation on a case by case basis depending on the gravity of issues and potential losses involved. The Internal Auditor will oversee and control the subsequent investigation, therefore for this purpose the Head of Investigation will report to the Internal Auditor.

» The Terms of Reference should be agreed between those involved in the investigation. The Head of Investigation should arrange for an action plan to be put in place with, as far as is possible, a set timeframe and regular reviews. He should call on the assistance of various sources of help at all stages (technical assistance, personnel, external audit, attorneys, etc.) but ultimate responsibility and accountability in progressing the case should remain with the Head of Investigation.

» The Head of Investigation should have the necessary authority (i.e. the appropriate rank and experience) to enable him/her to properly discharge these duties. Depending on the volume of work to be performed and

the issues involved, this person might be released from his/her main duties in the Company on a temporary basis.

» The Head of Investigation should also be independent from the matter in question. It is the responsibility of the Head of Investigation to keep the Internal Auditor abreast of developments and report all material developments promptly to facilitate onward reporting to the Executive Team and Audit Committee.

LEARNING FROM EXPERIENCE

Following completion of the case, the Internal Auditor should prepare a summary report on the outcome and lessons learned circulating it to all other interested parties who must take the appropriate action to improve controls to mitigate the scope for future recurrence of the fraud. Where a fraud has occurred, Management must make any necessary changes to systems and procedures to minimize prospects for similar acts of fraud.

SUMMARY

Deloitte, one of the world's largest business consultants, offers the following guidance for businesses that want to begin a fraud-response plan:

» Create an allegation system:

◊ In what ways does the company systematically receive complaints?

◊ What process exists to assess the validity of complaints?

◊ How does the company train team members on what they should do if they suspect fraud?

◊ How does the company train team members on what they should not do if they suspect fraud?

Allegation Triage:

» How does the company determine when to escalate a complaint to a formal investigation?

» How does the company document the criteria to determine which complaints get investigated?

» What protocols guide the investigator's assignment?

◊ Case Investigation:

» What work plan exists to guide investigations?

- How do investigators handle evidence?
- What level of competency do investigators have?
- How does the company review case status?
- Who has access to case files?
- Communication and Reporting:
  - How do investigators communicate with stakeholders?
  - How does the company reveal investigations to team members?

Action List

The following checklist of actions may guide a person that suspects fraud within the company.

1. Do not act on emotion. It's time to gather all the facts.
2. Alert appropriate management within your organization. This, of course, heavily depends on who's suspected of committing the fraud. Fraud discovered at the lower echelons of the company can probably be handled by the direct manager in association with the compliance supervisor. Things get a bit more complicated the higher you move up the corporate ladder. Accountability, though, goes straight to the President, CEO and Board of Directors. So, make sure compliance

is amply prepared and authorized to do what's necessary even upon discovery of high-level fraud with the company.

3. Document date, time and details of initial report/discovery. This is important for both the reporting of the suspected fraud and ongoing investigation.

4. Take notes (and/or pictures and video) of all observations and actions. Important information can quickly be forgotten or confused over time. Creating copious notes and/or documenting photographic evidence helps ensure you have all the information the company needs to maintain the integrity of the investigation.

5. Maintain confidentiality (only inform those people who need to know about the suspected act). Loose lips sink ships – and investigations. Prematurely alerting the suspect(s) leads to destruction of evidence and cover-ups.

6. Do not confront the suspect. You could be putting yourself in danger, in addition to undermining the investigation.

7. Write out in full the suspected act or wrongdoing in as much detail as possible, including:

   ◊ The alleged occurrence,

   ◊ Who was involved in the occurrence,

- ◊ Whether the activity is ongoing,
- ◊ Location of occurrence,
- ◊ The value of the loss or potential loss, and
- ◊ A list of who else may know of the activity.

Collection of evidence is critical for proving the crime. Corporate investigations can take months and legal ones even longer.

Identify and Document Evidence, such as:

- » Invoices,
- » Contract and Agreements,
- » Purchase orders,
- » Checks,
- » Computers,
- » Laptops,
- » Tablets,
- » Cell phones,
- » Cloud access accounts,

» Credit card statements, and

» Relevant social media accounts.

1. Immediately gather the evidence (only if doing so will not alert the suspects) and place it in a secure area. Bear in mind a need to maintain a legitimate chain of evidence in case it becomes necessary to bring in outside authorities.

2. Protect the evidence from damage or contamination. This includes all confiscated electronic devices. You may need the evidence for civil or criminal proof, or even use it in a countersuit should you need to against a litigious fired employee.

3. Identify all potential witnesses. This includes people within and without your organization. Certain people may even alternate from witness to suspect and vice-a-verse during the course of your investigation.

4. If possible, secure and/or remove the suspect's access to relevant computers and security systems. This decision is delicate and may need to be made at the highest levels of authority within the organization. There's a fine balance between mitigating damages and continuing to collect evidence. You may want to consult outside legal and accounting firms and request an Opinion Letter regarding your decisions, depending on the situation.

5. Ensure regular back-up of all files and secretly place additional security on all accounts the suspect(s) may have access to.

6. Contact the company's outside counsel and accountants for advice and recommendations. This should occur early on in the process but, typically, at the highest levels of management.

7. Contact the company's insurance carrier. You may or may not be covered for the type of fraud under investigation. Should you be covered, the insurer may have its own processes for conducting investigations and you may unwittingly forfeit certain rights or claims by not alerting them early enough. The insurer, moreover, may try to deny the claim and you might be forced to retain additional counsel to sue your insurer for coverage.

8. You may need to retain a forensic accountant. Some frauds can be quite elaborate and complex, involve multiple jurisdictions and/or require advanced training in computer programming. A full investigation may require particular expertise.

9. Continue to monitor suspicious personnel and activities to ascertain the full breadth and extent of the fraud.

What If Agencies Call?

Lesson 10

The best way to prepare for the events about to unfold is to know and understand what to expect.

Government investigators receive extensive training on how to question and interview people. They exploit opportunities to build a record that will lead to charges or further problems for witnesses, subjects, and targets of their investigations. Investigators specialize in developing and documenting evidence, while playing individuals against each other to elicit the narrative that suits their purposes.

A comprehensive compliance strategy will help a company manage the information and demonstrate a good-faith effort to comply with regulations and the law. By building a record of good-corporate citizenship, a company can show transparency and defend itself effectively in the investigators begin asking questions.

As described in earlier modules, government investigators do not act without having a specific intention. If they ask questions or subpoena documents, they likely already have invested thousands of hours and they believe they can build a case. When they start talking with people in a company, they want to gather more evidence. Their investigations will be in an advanced stage, but the witnesses may not know anything about the nature of the inquiry. Some investigators will try to intimidate or trap witnesses.

When initially approached, people that work for companies may get nervous. They may:

» Believe they didn't do anything wrong and act belligerently,

» Deny that they didn't do anything wrong and make statements that can hurt them,

» Accuse others within the organization in an effort to minimize culpability,

» Cooperate fully without knowing or understanding whether they are exposing themselves to legal complications.

If the company does not help team members understand the nature of an inquiry, those team members may get themselves and the company into deeper troubles. Remember that the investigators want to prevail. Victory for them means some type of sanction, injunction, disgorge-

ment, finding, or conviction. Investigators do not earn promotions by letting companies or individuals off the hook. On the contrary, their careers advance when their investigations lead to penalties. They may try to appear friendly, saying they only want the truth.

Yet people should always remember the wisdom of President Reagan, who warned of nine words that an American never wants to hear:

» I'm with the government and I'm here to help.

How Investigators Start:

The investigative team starts gathering evidence in a number of different ways. The investigators may identify an employee, a group of employees, or other potential witnesses. If the investigators believe the prospective witnesses will help them build a case against the target, they will conduct an interview—either with or without someone to transcribe the exchange. Since the investigators would have to give any transcriptions of the interview to the opposing parties during the "discovery" phase, they may elect not to take notes or recordings of any kind. Business leaders may or may not know that the government has begun an investigation.

Other times, the government agents may want to show force. In those situations, the agents make a surprise vis-

it, often loud, with an overwhelming display of firepower. Scores of people wearing dark windbreakers with large yellow letters (FBI, SEC, FTC, IRS, FDA, etc.) may show up to conduct a search.

Regardless of whether the government agents use subtle or strong-arm tactics, they always give a sign that more invasive activity will take place, putting a company and its employees in significant legal jeopardy.

The investigative tactics that the government agents use may dictate the appropriate response for people within the company. Our team at Compliance Mitigation offers insight that leaders may consider if they learn of:

» Informal employee interviews,

» Execution of a search warrant, or

» Grand jury subpoenas, or depositions.

Regardless of what approach the government investigators take toward a company or its employees, people should try to determine whether the agents consider the people or the company as:

» A witness to the investigation,

» A possible subject of the investigation, or

» A target of the investigation.

If a person can determine the government's posture toward the company from the beginning, that person can better assess the potential liability.

Our team at Compliance Mitigation encourages leaders of businesses to get competent legal advice—we are not lawyers and we do not offer legal advice. All of the information we provide comes from our experience of having gone through government investigations and having interviewed thousands of people that have gone through government investigations. We offer insight that business leaders may consider to protect themselves against being dragged into government investigations.

Experience convinces every member of our team that, despite sound business policies and internal audits, investigations can come unexpectedly. With thousands of regulations, people may operate a business that violates laws or regulations; ignorance of those laws or regulations, however, will not immunize them against an investigation.

On the other hand, regular training that shows a good-faith effort to comply with applicable statutes and regulations may limit a company's exposure. With our nation's commitment to big government and mass incarceration, we believe every business is vulnerable. Our team offers general guidelines, and real-life experience of what happens to people who get caught up in a government investigation.

Informal Interviews

Sometimes, agents will show up at a person's home, or approach a potential witness at some other non-threatening location. The agents may or may not advise the employee that the person has the right to decline to answer any questions. Also, the agents may inform the person that anything the person says could possibly be used against the person later. As a result, people who are not prepared to respond to a government investigator may consent to the interview, not knowing that he or she has the option to refuse.

If a government investigator approaches any citizen, the person may feel nervous. After all, if the investigator believes the person lied, the investigator may initiate criminal charges for lying to an officer.

Further, that conversation could lead to enormous legal costs in the event that the government subpoenas the person for a deposition later. People who lack preparation or knowledge may not recall details when responding to

questions; government investigators can twist words, or later use a person's words to malign, or cast doubt on the person's character.

A company should take proactive measures to prepare people for the possibility of a government investigation. It should also provide general training about a person's rights in the event that a government agent asks for an interview. That training should include instructions, or options, that an employee may consider if approached by an agent. Some guidelines on training may include what a person should do if:

1. Employee informs company that a government investigator wanted to speak with him or her:

If an employee lets the company know that a government investigator made contact, the company may want to hire an attorney for the employee. The attorney may speak with the prospective witness to talk about rights the person may have. A prospective witness may decline to speak with the investigator, or the witness may choose to have an at-

torney present. The company's lawyer may try to intervene and ask if the questions pertain to the company; if so, the company's lawyer may ask for an opportunity to attend the interview with the witness.

2. The witness speaks with the government, but the company doesn't know until after the interview:

If the company learns about the interview after the witness spoke with investigators, a lawyer should attempt to speak with the employee. Neither the company's lawyer, nor anyone else, should make the person feel as if speaking with the government violated anything at all. By speaking with the employee, the lawyer should attempt to learn the substance of what the government wanted to know.

Although the lawyer may advise the employee of his or right to counsel, no one should retaliate against the person in any way. Any type of retaliation or judgment could work against the company, potentially eliciting accusations of violating whistleblower statutes or obstruction of justice charges.

3. The company should prepare employees whom the government may target for interviews.

The best time to prepare for a government investigation would be before the government investigation begins. In other words, our team at Compliance Mitigation encour-

ages leaders to train for best practices, consistent with the compliance manual. That training should include guidance for people to consider in the event that government investigators target them.

1. The company should help all employees understand their rights to counsel, and their rights to refuse to speak with investigators.

2. Training should include real-life stories of people who have been dragged into government investigations, showing the disruption those investigations can cause.

3. The company should never advise employees to hide, deceive, or mislead a government investigator; they should also train on the penalties that can follow for a person if the investigators accuse the person of lying.

4. Although government agents may use their authority to intimidate people into talking, a person has the right to refrain from saying anything to a government investigator.

5. If a person talks with a government investigator, and the investigator accuses the person of lying, the government may charge the person with a federal crime that could result in a five-year prison term.

6. A person has the right to have counsel present if he or she talks with a government investigator.

7. If a person hires a lawyer, that lawyer will represent the person and not the company. The conversations a person has with the lawyer of record will remain between the client and the lawyer—unless the person authorizes the lawyer to share the information with others.

If Authorities Execute a Search Warrant

Although investigators may interview witnesses in private, trying to keep their inquiries under wraps, sometimes they choose a more intrusive approach to let the company, the company's leaders, the media, and other businesses know that the company has become the target of a government investigation. Together with a law enforcement agency, like the FBI or the local sheriff's department or police department, a cadre of officers may burst into the business. In those instances, the officers yell for everyone in the office to step away from the computers and stop what they're doing.

When law enforcement officers execute a search warrant, they may be loud and intimidating. The people work-

ing in the office will likely not know what constitutional protections exist. For this reason, the company should train people on important steps they can take to protect themselves.

Rules that Govern Search Warrants

If investigators have gone to the trouble of getting a search warrant, it's safe to assume that they intend to bring charges that will disrupt the company and the lives of many people that work in the company. The warrant differs from getting a subpoena, which authorizes the investigators to obtain documents or recordings voluntarily.

To obtain a search warrant, the investigator must persuade a judge that the government has probable cause to believe that evidence of a crime exists in the location. The target of the warrant will not know that the investigator is communicating with the judge. As such, the target cannot work to defend against the argument that the investigator will make to the judge.

To show probable cause, the investigator may rely upon evidence gathered through an affidavit, recited under oath, that shows the reason(s) the government believes the target has participated in a crime. The warrant must define places to be searched, the people the investigators want to search, and the types of things the investigators wants to seize.

According to Rule 41 of the Federal Rules of Criminal Procedure, once a judge issues the warrant, the investigators have ten days to serve the warrant. In most cases, the officers show up between 6:00 am and 10:00 pm. The agents must provide the company with a copy of the warrant, and also with an inventory list of everything they've seized.

» During training, the company should explain how such warrants may result in officers taking personal cell phones or devices that contain personal information, including emails and text messages. All of this information can lead to the expansion of government investigations.

Investigators exercise search warrants when they want to catch a company and its team by surprise. A company can mitigate this disruption through appropriate training and preparation at various stages of the investigation—including, before, during, and after. Our team at Compliance Mitigation provides that specialized training.

What Happens During a Search?

Good training may protect the company against the shock and awe of a team of government agents executing a search warrant. Expect those agents to be loud and act aggressively as they try to show absolute control over the scene.

The agents will likely gather the employees together and relegate them to a specific area of the business. These tactics can shake people into fear and induce some to cooperate in ways that go far beyond the scope of the search, which can expand the investigation.

Company leaders should prepare employees for what happens in a search, and how people may want to respond. If a search takes place, a company representative should ask to see a copy of the search warrant and also the identifying credentials of the people searching.

It may make sense for the company to assign a "warrant team" to represent the company in the event of a surprise search warrant. People on the warrant team may have higher levels of training, so they can keep people calm and potentially limit the intrusiveness of the government investigation. The designated leader of the warrant team may want to take the following measures in the event of a surprise search warrant:

1. Contact the company's designated attorney and corporate leader—which means the team leader should have the appropriate people's contact information.

2. Request that the agents postpone the search until counsel arrives.

3. Request identification from the people on the search team.

4. Review the warrant and, if available, the affidavit the investigators used to persuade a judge to issue the search warrant.

5. Ask the agents not to begin the search until after they have provided the warrant; although the agents will resist, the request may preserve rights to challenge procedures during later proceedings. A thorough review of the search warrant and possible affidavit may help the leader request that the agents confine their search to the precise scope authorized by the warrant.

6. Proper training may help the leader recognize defects in the warrant, such as a failure to describe the premises to be searched, or what the agents may seize, or the lack of a signature by an appropriate judge.

7. The leader may ask the agents for an opportunity to confer with counsel prior to the start of the search to determine whether the warrant has any defects. If the leader finds defects in the warrant, the leader should point the defects out to the agents and object to the search. Although the agents will likely continue, the objection may preserve the company's rights. The team leader should go on record to say that the company objects to the search.

8. The team leader should have some level of training on the Fourth Amendment of the Constitution, and how Courts have ruled that warrants must describe plac-

es to be searched and things that agents can seize. The team leader should have training that will empower the leader to understand what the agents can and cannot do.

9. The team leader should request the agents to provide an inventory list of everything they've seized.

10. If the agents come with a surprise search warrant, the team leader should advise all employees of their rights. Remind people that they have a right to counsel, and if they choose, they may remain silent. Perhaps the leader could direct employees to a link of a cloud-based statement of rights that they may access through smart phones.

11. The leader should strive to protect privileged information that should belong to the company and its law firm.

12. The leader should strive to monitor the search and record the agents' activities. A good leader may take thorough notes. By memorializing the areas where the agents searched and the materials the agents seized, the leader may provide information that can assist counsel later. Include date and time and any other observation that may be helpful to memorialize the search. If the agents object to video cameras, the team leader should ask the agents to state objections formally to counsel.

13. The company may have the right to record the search by any means, so long as recording does not interfere with the agents' duties. There isn't any reason why unobtrusive videotaping, audio taping, or photography would interfere with a search. But since the agents are so intimidating, an untrained workforce may not think to record.

14. Team leaders should not put themselves at risk of being arrested by the law enforcement officers for obstructing the search.

15. Team leaders should request that the agents make copies of any electronically stored materials, rather than removing computer hard-drives, or other computers from the office. The team leader must know how to get back-up materials. If possible, the leader should attempt to coordinate with the agents so that the results do not completely obliterate the business's ability to operate. The company's attorney should provide specific language the leader may use to preserve all of the company's rights.

16. After the search, the team leader should provide a full report to the company's attorney.

Training Topics the Company Should Include:

1. Help all team members understand that, although unlikely, all businesses are subject to government investigations.
2. Help all team members understand a search warrant and what they should know if authorities execute a search warrant.
3. Show a cloud-based system that provides reminders of what people should do in a search warrant and let the people know how they can access the information on a smart phone.
4. Identify the warrant team and provide specialized training for team leaders.
5. Show how to monitor agents and record notes.
6. Show that although the company intends to cooperate with the investigation, the team leaders want to preserve rights for people and for the company.
7. Emphasize that employees should not impede the search, conceal or destroy documents.
8. Explain appropriate laws, including obstruction of justice and making false statements.

9. Train employees on the rights regarding government interviews.

10. Create a "Policy and Procedures" for team leaders to know how they should respond to search warrants, including:

- ◊ Information and instructions on contacting counsel and company leaders, with contact numbers.
- ◊ Request the agents wait until counsel arrives before conducting the search—understanding that the agents do not have an obligation to wait.
- ◊ Ask the agents for identification.
- ◊ Ask for a copy of the warrant.
- ◊ Send an image of the warrant to the company's attorney.
- ◊ Expressly state that although the company will cooperate, it does not consent to the search.
- ◊ Direct all employees to the document that explains their rights with regard to being interviewed.
- ◊ Review the warrant and attempt to negotiate terms of the search.
- ◊ Do not remove, discard, or hide any objects that might be subject of the search warrant.

- ◊ Carefully monitor any search.
- ◊ Ask the agents to permit you to photocopy any original document that the agents seize.
- ◊ Get a receipt for any files or property the agents seize.
- ◊ Do not conduct any meetings with employees without an attorney present.

Subpoenas, Grand Jury Investigations, Depositions

Although a government search is immediate and catches people by surprise, investigators can rely upon other tactics to gather evidence against a company and its leaders. On the surface, subpoenas may seem less intrusive, because agents aren't coming in with loud fanfare. But subpoenas, grand jury investigations, and depositions can be extremely invasive and broad.

The agents may not need probable cause to convene a grand jury or to issue a subpoena. The requests may be extremely broad, asking for information that is difficult to produce—like records going back several years, or all email and text exchanges, or bank records and tax records.

Although witnesses will have substantial advance notice to comply with requests for the production of documents or testimony, such requests come with enormous liability. Failure to comply can result in charges for obstruction

of justice. For this reason, the company and the employees should consult with counsel if they ever receive a subpoena. Further, the company should provide basic training to help all team members understand the process and implications.

Conclusion:

The best time to protect a company would be before a government investigation begins. For this reason, the company should engineer a compliance and training program that identifies all corporate policies, processes, and procedures, pertaining to every aspect of the company. The company should have excellent, cloud-based record-keeping systems in place, and potentially a Customer Relationship Management software system that maps out the entire company journey, including:

- A staff hierarchy with clear job descriptions, responsibilities, qualifications.
- A staff training system that articulates the corporate culture.
- A process map that shows how the company operates.
- The customer acquisition strategy, including all advertisements and lead-generation systems.

- The scripts or training that sales teams use.
- Templates for all invoices and contracts.
- Effective financial records that document every transaction.
- Warranties, representations, and company communications with customers.

Transparency can protect an honest company and its leaders from the enormous cost of a government investigation. With good training, the company can also protect itself in the event that something goes wrong, which could bring unwanted attention from government investigators.

Strengthening Compliance

Lesson Eleven

To design a successful compliance program, start by guidelines set forth by the Department of Justice. But don't stop. To strengthen the program, we recommend that leaders review programs that failed for other businesses. Good critical-thinking skills will lead to modifications and continuous improvements.

Get buy-in on a compliance programs importance from all team members, and from corporate leadership. As the cliché holds, leadership starts at the top. A company could include all the Department of Justice's requirements, but it will fail without buy-in from team members and leadership.

Government regulators and investigators make it clear that they expect companies of all size to operate in compliance with laws and regulations. Mega-cap companies like Facebook, Google, and Amazon face investigations, just as investigators may target mom-and-pop companies for violations of laws or regulations. Learn what happened to others. Use those lessons to improve compliance programs to protect businesses and team leaders.

Companies primarily adopt compliance programs because they recognize the need to mitigate risk. Leaders want to get the end result of a safer workplace with less legal exposure. Merely adopting a compliance program, however, without comprehensive implementation, may not yield the return on investment that a leader wants.

On any given day, we can turn to the Department of Justice website to read press releases of criminal indictments for white collar crime. Many of the defendants in those cases began without any intention to break laws. Yet a lack of a clearly defined business model, or well-engineered compliance system, put those people into the cross hairs of a government investigation. High legal costs and criminal proceedings followed.

All businesses stand vulnerable to the dangers of a government investigation. For these reasons, leaders should take steps to minimize their exposure. That means they should put plans in place to show a commitment to transparency, compliance, and good corporate citizenship.

Our team at Compliance Mitigation has identified 10 reasons that compliance programs may fail in businesses:

A Failure to Appreciate Risk

Leader should begin with an honest assessment of the risks the company may face. To get the right answers, they

may ask Socratic questions. Rather than starting from the perspective of the company leader, questions should come from the mindset of an investigator. Those people will be cynical. If company leaders do not anticipate such questions, they may fail to appreciate their exposure to risk.

Company leaders frequently strive to:

» Provide products or services to satisfy customer needs,

» Create jobs and paychecks for employees,

» Contribute to the building of stronger, more vibrant communities, and

» Earn an acceptable return on investment for shareholders.

A company may not have the luxury of hiring an entire team or department to contemplate risk exposure. Yet if they do not understand the risk, they may not see value in a compliance program. If leaders do not see how a compliance program can strengthen the overall health of the organization, they may undermine its effectiveness. Without a good compliance program, the company and its team leaders may face harsher scrutiny from regulators and investigators. For these reasons, proper training should highlight failures and the accompanying costs of a bad compliance program.

Lack of Leadership Buy-In

When it comes to compliance, leaders should recognize that the company's commitment to ethics starts at the top. If leaders do not embrace the principles of good conduct, team members will not take compliance seriously.

Compliance programs that send mixed or inconsistent messaging leave the company vulnerable to liability. That liability can include exposure to internal fraud, lawsuits from customers, investigations by government regulators or law enforcement.

Good training should profile examples of the fallout that has come from such failures in compliance.

A Paucity of Resources Devoted to Compliance:

Failing to devote financial resources to support compliance training exposes a company to more risk. If an investigation begins, and the company cannot show a deliberate, consistent investment in the pursuit of excellence, authorities will be less likely to see the business or its leaders as good actors. On the contrary, investigators may accuse the business and the responsible parties of operating from a state of "*willful blindness,*" a term we heard a lot about while our team members were in prison.

Compliance training does not have to be a drain on the company's resources. In fact, when leaders design compliance programs to demonstrate a commitment to transpar-

ency, they may be simultaneously investing in corporate messaging. That better messaging can lead to better efficiencies, helping every team member get a full grasp of how the company operates and achieves excellence.

With such a commitment, every team member may work collaboratively, in accordance with corporate goals. When leaders view compliance as an essential part of the corporate mission, they devote the appropriate resources. Those resources may advance corporate success, while simultaneously mitigating risks.

Demoralizing Compliance Departments

When company leaders view compliance programs as being wasteful expenses, team members won't take the program seriously. Unfortunately, if anything should ever happen that brings the company to the attention of government investigators, leaders should expect to pay a heavy price.

Clearly, a company succeeds by devoting resources to sales teams, marketing teams, and operational teams that build thriving businesses. Yet leaders should model themselves after athletic coaches that require players to train on fun-

damentals. Coaches invest in defense and offense, not just offense. Likewise, business leaders should invest in defensive measures that will protect all team members.

If a government investigation begins, the value of an effective compliance program will become readily apparent. On the other hand, a demoralized or feeble compliance program will only hurt the organization. Government attorneys will use flawed policies as evidence of the company's devotion to willful blindness.

Indeed, the Harvard Business Review published an article describing how the Department of Justice tasks prosecutors "to determine whether a corporation's compliance programs is merely a 'paper program' or whether it was designed, implemented, reviewed, and revised, as appropriate, in an effective manner."

» https://hbr.org/2018/03/why-compliance-programs-fail

The Policies Lack Clear Instruction and do not Relate to the Business

A good compliance training program engages team members. If leaders do not supplement off-the-shelf compliance programs with additional instruction that teach or inspire team members, they miss an opportunity.

Neither boilerplate language, nor dense legal jargon, will help. An option would include supplementing training exercises with human case studies. Leaders may profile the story of a person convicted of a white-collar crime. Task participants with identifying what went wrong. Perhaps encourage them to come up with strategies that may have lessened the risk. Use the feedback as a resource to strengthen corporate processes and procedures. Another option would be to create cloud-based, on-demand video training that encourages the development of critical-thinking skills.

Misplaced Incentives

A company can doom a compliance program by failing to align compensation with good corporate behavior. If a company incentivizes people to get sales by any means necessary, they may simultaneously create a culture of non-compliance. Many people serve prison sentences for violating laws related to:

» Foreign Corrupt Practices Act

» Sherman Antitrust Laws

» Money Laundering

» Identity Theft

» Bribery

» Mail Fraud

» Wire Fraud

» Honest Services Fraud

» Securities Fraud

While in prison, many of those people complain that they only did what their companies wanted them to do. The employees lost, and in many cases, the companies lost as well—paying enormous financial penalties. Good compliance programs will incentivize excellence in every area, providing training that shows a commitment to good corporate citizenship.

Inadequate Communication and Training

Corporate leadership requires clear and consistent messaging that shows how leaders define excellence. Leaders that do not communicate the company's commitment to integrity give license for other people to violate rules. The training should show that the company places a high value on excellence—and placing a high value on excellence means training for excellence in communications, from the top down.

The communication channels should flow both ways. People at every level in the organization should have an opportunity to ask questions or express concerns. If an employee sees something wrong, the person should have some

mechanism to speak up without fear of retaliation. Without that two-way communications and training, the company may weaken a compliance program.

Outsourced Noncompliance

A company cannot escape punishment from law enforcement, or escape liability from regulators, by outsourcing noncompliance. Both the Department of Justice and regulatory agencies have launched government investigations that punished entities for contracting with outside contractors or third parties that facilitate illegal behavior. Further, when leaders look for plausible deniability by using the "it's-not-my-fault" defense, they expose themselves to accusations of being willfully blind to illegal or corrupt behavior. Bad and inconsistent messaging threatens the entire the organization.

Failing to Monitor or Audit Compliance

If the company doesn't show a commitment to maintaining compliance, the team members will ignore the training. They may do what is necessary to pass an internal quiz on what they have learned. As soon as they leave the training session, however, many of those people go about business in a manner that shows a total disregard for what the compliance program ostensibly teaches.

In contrast, a company with a true commitment to compliance will show team members how the company's leadership invests heavily in corporate excellence. Besides ongoing training, they may show a commitment to monitoring by sponsoring a private "hotline" that encourages people to report noncompliance. They may conduct internal audits or perform phantom calls to see how people will respond. Then, the company may announce its findings regularly.

When team members understand that the business's leaders monitor and audit compliance, people will show more commitment to operating in harmony with what they've learned through compliance training.

Inconsistent Enforcement and Discipline

If a company is harsh on low-level employees, but it allows rainmakers or leaders to get away with noncompliance, the compliance program will fail as a resource to protect against government investigations. As the above-quoted *Harvard Business Review* article noted, prosecutors will deal harshly with companies that do not treat the compliance program as an integral part of the organization

To grant a non-prosecution agreement, prosecutors will assess the company's policies—including records the company keeps on disciplinary or corrective measures for noncompliance.

The following 20-page report that the Department of Justice published will help leaders grasp the "critical factors" prosecutors will use when assessing "the comprehensiveness of the compliance programs."

» https://www.justice.gov/criminal-fraud/page/file/937501/download

That document shows a compliance program should provide a clear message that leadership will not tolerate misconduct. The program cannot succeed if prosecutors determine that policies do not apply to people in senior leadership positions. According to the document:

"The company's top leaders set the tone for the rest of the company. Prosecutors should examine the extent to which senior management have clearly articulated the company's ethical standards, conveyed and disseminated them in clear and unambiguous terms, and demonstrated rigorous adherence by example. Prosecutors should also examine how middle management, in turn, have reinforced those standards and encouraged employees to abide by them."

Compliance 101

Avoiding Government Investigations and White Collar Crime

Our team at ComplianceMitigation.com helps business leaders and their teams make decisions to avoid government investigations and charges for white-collar crimes.

The Department of Justice encourages business leaders to support well-designed compliance programs that work in practice.

With our compliance programs, your team members will learn how to make better decisions, minimizing vulnerabilties to costly government investigations and charges for white-collar crimes.

Team@ComplianceMitigation.com

949-205-6056

Larry Hartman

Michael Santos