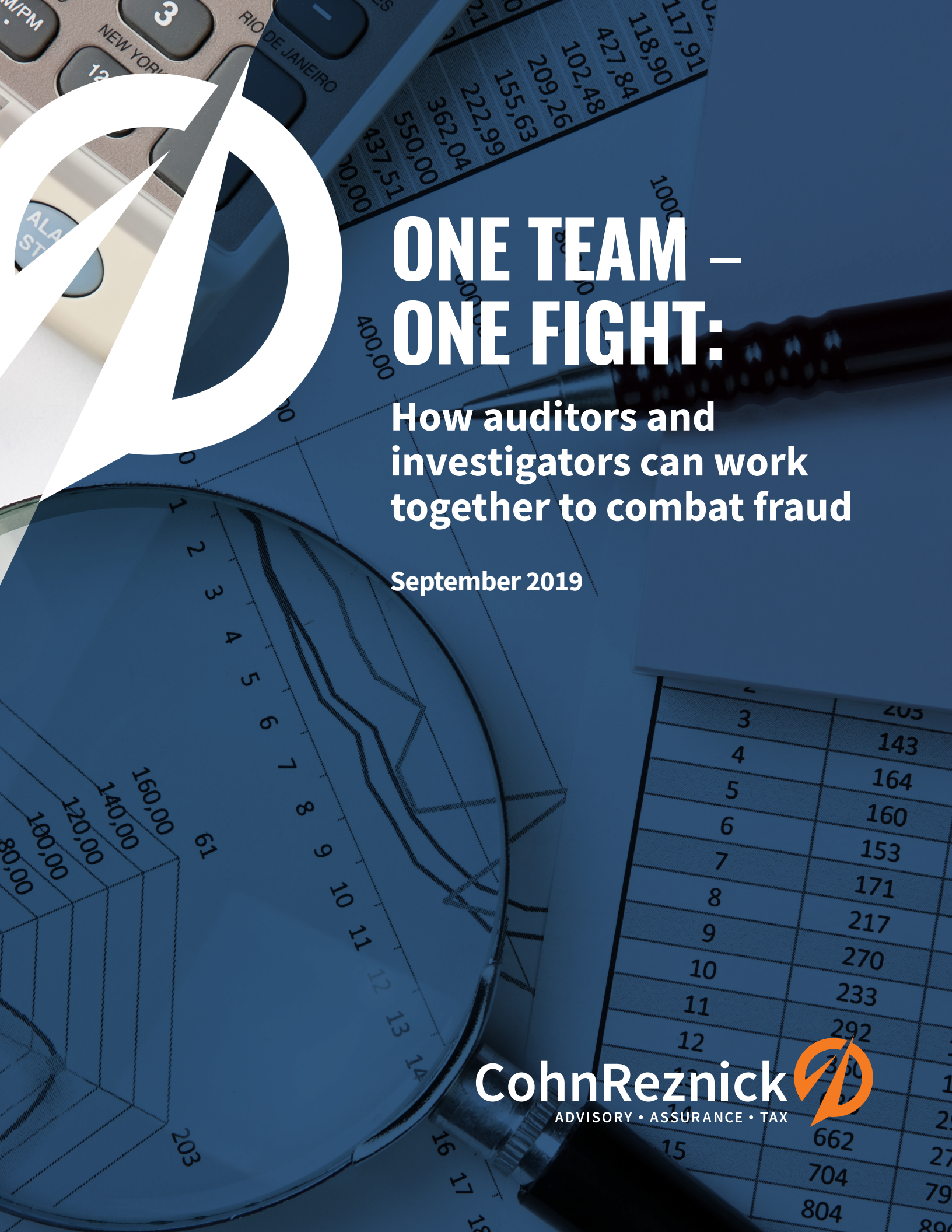


ONE TEAM – ONE FIGHT:

How auditors and investigators can work together to combat fraud

September 2019

CohnReznick

ADVISORY • ASSURANCE • TAX

TABLE OF CONTENTS

PREFACE

"One Team-One Fight" is a slogan borrowed from the armed forces. It speaks to the idea that when soldiers, sailors, marines, and airmen bond as a team, there is nothing our fighting men and women cannot do to protect our country and liberty. The same "One Team-One Fight" model also applies to auditors and investigators. The more they work together, the more successful and formidable they become at combatting fraud.

CURRENT TRENDS IN FRAUD DETECTION

According to the Association of Certified Fraud Examiner's (ACFE) Report to the *Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study*[1], the most common means of fraud detection is "tips," i.e., the voluntary reporting of potentially fraudulent acts. Tips account for nearly 42% of all fraud detections[2]. In fact, tips have consistently been the most common means of fraud detection since the ACFE began tracking this data in 2002[3]. Employees account for nearly half of all tips that lead to the discovery of fraud.

This statistic underscores the importance of organizations maintaining rigorous tip lines—or what is referred to in government organizations as "hotlines"—since organizations with hotlines are far more likely to uncover fraud from a tip. The second and third most common means of fraud detection are management reviews and internal audits, respectively. When combined, these account for about 30% of all fraud detections[4]. Management reviews and internal audits are similar except that audits must be performed in accordance with Generally Accepted Auditing Standards (GAAS)[5]. What is also noteworthy from the ACFE report is that law enforcement and external audit detect fraud at a rate of about three percent each[6]. The low fraud detection rate by investigators is attributable to the fact that their rightful role is to arrive at the scene of a fraud after detection and carry out the process of law enforcement.

COMBATTING FRAUD: THE POWER OF COLLABORATION

There are two opportunities any audit or investigative organization can take advantage of to detect and deter fraud. First, auditors and investigators should establish a synergistic relationship in which each discipline capitalizes on the diverse skill sets each possesses to collaboratively fight fraud. Second, investigators and auditors should leverage the vast resources offered by the ACFE to further enhance their knowledge and skills in combatting fraud. By combining the strengths of audit and investigative organizations while also applying the state-of-the-art fraud fighting techniques provided by the ACFE, fraud detection resulting from management reviews (16%), internal audit (14%), and law enforcement (2%)[7] can be significantly increased.

---

[1] Association of Certified Fraud Examiners, *Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study.* (http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf.)

[2] ACFE, *Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study*, page 19.

[3] Ibid.

[4] Ibid.

[5] Statements on Auditing Standards, American Institute of Certified Public Accountants, Inc.

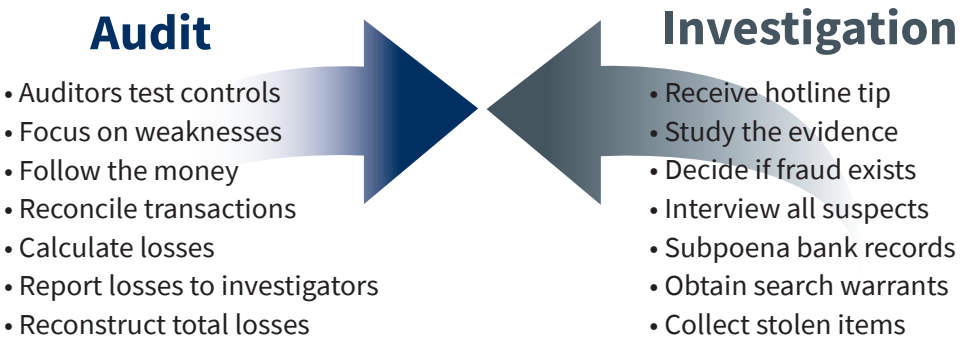
[6] ACFE, *Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study*, page 19.

[7] Ibid.

HOW AUDITORS AND INVESTIGATORS CAN PLAY TO EACH OTHER'S STRENGTHS

To begin a discussion on how internal auditors and investigators can effectively use internal audit, management reviews, and investigations in combination to combat fraud, a description of each is helpful.

COLLABORATION—HERE'S HOW IT WORKS



Internal audits

As defined by the Institute of Internal Auditors, *"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes[8]."* Furthermore, *"internal auditors' roles include monitoring, assessing, and analyzing organizational risk and controls; and reviewing and confirming information and compliance with policies, procedures, and laws. Working in partnership with management, internal auditors provide the board, the audit committee, and executive management assurance that risks are mitigated and that the organization's corporate governance is strong and effective. And, when there is room for improvement, internal auditors make recommendations for enhancing processes, policies, and procedures[9]."*

[8] Institute of Internal Auditors, "Definition of Internal Auditing"

[9] Ibid.

Management reviews

A management review is similar to an internal audit in that it involves an examination of an entity's operations or transactions with the intent of providing recommendations for improvement. However, what distinguishes a management review from an internal audit is that it usually does not comply with GAAS. Management reviews are often "ad hoc" in that they are performed because of an emergent issue regarding potential fraud, a loss of inventory, a shortage of cash, a security lapse, etc.

For example, a management review team may consist of personnel who are not qualified to perform audits but possess unique knowledge and expertise of the subject being reviewed. Often, however, the members of a review team are not sufficiently independent from the topic being reviewed to comply with GAAS. Thus, a review team may limit the scope of their examination to exclude adequate testing of internal controls to meet the auditing standards.

In essence, management reviews are often limited to small numbers of transactions usually insufficient in number to opine on the adequacy of internal controls, are restricted to focus only on noted vulnerabilities, and performed by personnel whose professional skills are other than audit. The value of a management review is fast response, being able to assign personnel when auditors are not available, and streamlining reviews to only target suspicious transactions—and with such limitations as to not express an opinion on an internal control environment.

Investigations

An investigation involves a detailed examination of activities with the goal of determining whether laws were broken. Investigations are conducted on individuals, companies, or organizations suspected of engaging in illegal activity. Investigative staff consists of trained, credentialed, and sworn law enforcement officers (criminal investigators), investigative attorneys, and administrative investigators[10]. These investigators are focused on determining the legality of conduct engaged in by persons suspected of committing fraud whereas internal auditors are focused on examining transactions and accounts in order to prove the accuracy and fairness of the operating results and financial position of a business.

Unlike internal auditors, investigators are empowered to make arrests, seize physical evidence, and prepare evidence for prosecution. Investigators bring fraudsters to justice by focusing on intent, an essential element to proving a fraud has been committed. Because auditors are skilled at transaction examination, investigators often request their assistance for such activities as recreating inventory balances to determine the amount of losses or reviewing controls to identify the scheme a fraudster used to syphon off cash or material. After a criminal investigation or conviction, investigators will provide auditors with the circumstances that uncovered the fraudulent activities. Auditors can then conduct a fraud risk assessment or be on the lookout for similar criminal activities at other locations.

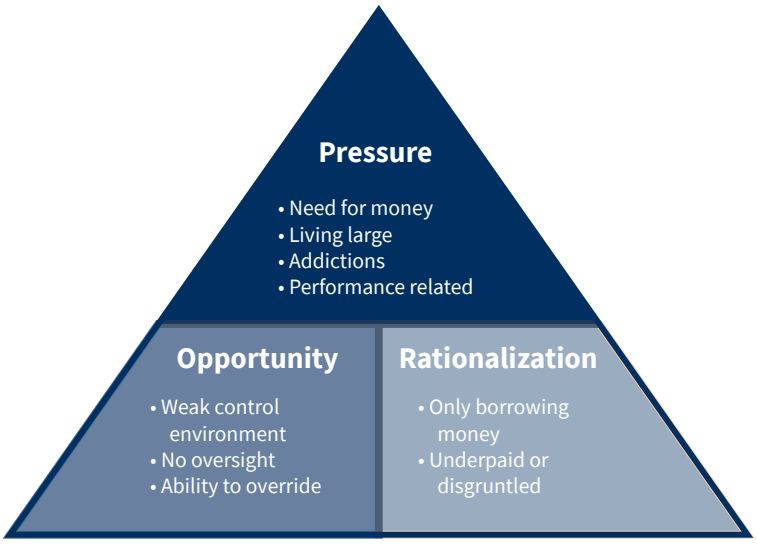
In summary, investigations are carried out by members of law enforcement to determine whether specific allegations, complaints, or information point to possible violations of law, regulation, or policy. The role of investigators encompasses a variety of matters, including investigations of fraud involving grants and contracts, administrative irregularities, employee misconduct, bribes and kickbacks, product substitution, and other issues concerning ethics and law compliance. Investigators build their cases on standards of evidence that are not required to meet GAAS. As effective as the tips and hotlines are for detecting fraud, it is the investigators who turn those tips into prosecutions.

[10] The Office of Inspector General (OIG), Department of Commerce, "Who Conducts OIG investigations?"

RED FLAGS: PROFILE OF A FRAUD PERPETRATOR

According to the ACFE, fraud perpetrators often display warning signs that indicate they are engaging in illicit activity. Thus, many fraud audits and investigations start with an examination of the common factors that cause people to commit fraud.

THE FRAUD TRIANGLE



Pressure

- Swimming in debt
- Celebrity lifestyle
- Legal problems
- Gambling
- Drugs
- Unrealistic targets

Opportunity

- Careless tone at the top
- No transparency
- Weak control environment
- No auditing
- No separation of duties
- Limited oversight

Rationalization

- Disgruntled
- Denied promotion/bonus
- Worked extra hours
- Staff layoffs
- "My boss does it"/cultural

Developed by the late Donald Cressey, Ph.D., an American criminologist, the Fraud Triangle represents a long-standing theory that three factors must exist for an individual to commit fraud[11]. These factors are pressure, opportunity, and rationalization. Pressure speaks to an individual's chronic need for money (i.e., gambling addiction, legal troubles, lifestyle, etc.). Opportunity refers to an individual realizing fraud is possible because of a weak internal control environment (e.g., lack of separation of duties). The third side of the triangle is rationalization, which is often exemplified by individuals who believe that they are only going to "borrow" the money or that they are somehow entitled to it because they have been unfairly treated. Often, fraudsters are disgruntled employees who rationalize their misdeeds because they are convinced management has wrongfully denied them a promotion or other benefit—their act of fraud is righteously justified. The Fraud Triangle illustrates the three factors that, when taken together, increase the likelihood of an individual committing fraud.

[11] Association of Certified Fraud Examiners, "The Fraud Triangle"

Pressure

The most common behavioral red flags displayed by perpetrators are when they live beyond their means (44% of cases) or experience financial difficulties (36% of cases)[12]. Often, financial difficulties stem from gambling or drug addictions, seeking a lifestyle and luxuries beyond one's means, and legal difficulties such as divorce, delinquent debt, etc. Other profile factors of fraudsters include disgruntled employees who want to get even for not getting a promotion or pay raise.

Unfortunately, unless an appalling lifestyle of drug addiction or financial ruin is noticed and reported by a co-worker or Human Resources, investigators and auditors are unlikely to have knowledge of someone's lifestyle—good or bad. Thus, the "pressure" side of the Fraud Triangle is not part of any internal control testing. In addition, investigators do not snoop into someone's private lifestyle unless alerted of possible violations of law.

Opportunity

Opportunity is often the result of a weak internal control environment and thus is the one factor of the Fraud Triangle that internal auditors can identify during an audit.

A solid set of internal controls provides reasonable assurance that an organization's reputation, operations, and resources are safeguarded and that risks to its continuity are mitigated. The individual values, ethics, integrity, and competence are part of the entity's environment. The most important internal control is the tone at the top of an organization.

Management's tone serves to promote ethical core values for its people and is the basis for an organization's application of internal controls, providing standards for inspiring integrity, structure, and accountability. The tone at the top will support the role of internal audit, advocate thorough control testing, and act promptly to fix internal control weaknesses. There are many opportunities or control weaknesses that may lead to fraud. Some common examples of control weaknesses include a lack of separation of duties, inadequate supervision to ensure approval over payments and collections, lack of record-keeping, and missing or illegible receipts.

In addition, today's accounting systems and financial reporting are universally computer generated, which further facilitates financial statement fraud as well as fictitious accounts. Thus, internal auditors need to be skilled in controls testing to provide assurance that the opportunity to commit fraud is mitigated. One of the best sources for keeping up to date with the latest fraud detection techniques is the body of knowledge maintained by the ACFE.

Rationalization

According to the ACFE's *Report to the Nations on Occupational Fraud and Abuse*, the majority of fraudsters do not join an organization with the aim of committing fraud[13]. However, changes in personal circumstances or pressures to meet aggressive business targets often create the backdrop for their crime, especially once they are comfortable in their job and enjoy the trust and respect of colleagues. Many frauds begin at very low dollar values as the fraudster rationalizes they will pay the money back. But, as the perpetrator begins to realize no one notices, the temptation to take more and more money often grows and the rationalization morphs from "I will pay it back" to something such as "the owners are taking advantage of me because they do not pay me what I am worth." It is also likely that perpetrators begin to believe their fraud will never be noticed.

[12] ACFE, *"Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study,"* page 59.

[13] Ibid, page 52.

CHARACTERISTICS OF AN ORGANIZATION SUSCEPTIBLE TO FRAUD

There are three company/management profile factors that, when existing within the culture of an organization, unnecessarily expose it to fraud risk. These are organizational conceit, hypersensitivity, and obsessive cost cutting.

Organizational conceit

This occurs when leadership or management conceit sets a counterproductive and egotistical tone at the top. Typically, these leaders believe that they are running the most efficient and effective organization possible and everything is operating at peak performance, morale is high, and the stockholders or owners are happy with constant good news, albeit never independently tested. Such leaders willingly certify that controls are in place and operating effectively, even though their assumptions are based on unaudited self-reporting.

They tend to have low opinions of internal auditors and view internal audit as a waste of time and money. In their minds, internal control testing is a ploy for auditors to create self-generating business opportunities. These leaders surround themselves with "yes" men and women who will tell them what they want to hear instead of what they need to hear. Therefore, even if someone in an organization suspects fraud or theft, they will not report it for fear of a hostile response. As a result, these conceited leaders are shocked when auditors and investigators report fraud committed by their most loyal followers.

Hypersensitivity

Hypersensitive leaders are the opposite of conceited leaders. They lack self-confidence, are paranoid, and are obsessed with controlling any message about their performance. While hypersensitive leaders may allow auditors to work in their organizations, they will attempt to control the audit message because they fear the consequences of negative findings by auditors. They become so obsessed with reporting favorable results that they will attempt to coerce the auditors into softening or altering their findings, thus potentially impairing auditor independence.

In this kind of environment, subordinate employees do not trust their leaders to look out for their interests, creating an atmosphere aptly described as "every man for himself." The result is a weakened control environment filled with paranoid, untrusting leaders who are obsessed with projecting the right image to the owners or stockholders.

Obsessive cost cutting

A key element of any organization's process for continuous improvement is the reduction of unnecessary costs. However, some managers are so convinced of their ability to effectively cut costs that vital indirect or overhead functions — including auditors, comptrollers, and buying agents—are eliminated.

These managers often view internal controls as another source of waste because they require a larger payroll to ensure sufficient numbers of personnel are available to confirm the separation of duties, safeguarding of assets and IT controls, or accounting for funds. The managers prefer to cut costs and rely on their own self-reporting of good news instead of paying an auditor to independently report control weaknesses.

In the Department of Defense, there is a continuous drive to redirect resources from behind the lines to the soldiers on the front lines. This drive to support the front-line soldiers is commonly referred to as a "tooth to tail[14]" scrub of all resources to ensure there is maximum support for the men and women on the battlefield (tooth) and minimal waste on the support side (tail). Who can argue this concept as it is of paramount importance that soldiers have the resources they need to prevail? However, cutting the tail too much leaves the support activities vulnerable to fraud, waste, and abuse. While the drive to cut costs is often a noble pursuit, for many managers it becomes a badge of honor to reduce costs even if there is no strategic analysis to ensure the cost cutting will not jeopardize the safeguards against fraud, waste, and abuse.

Whenever there is a top-down initiative to reduce costs, efforts to streamline a process should be closely monitored because key controls may be eliminated. For example, if a dollar value checkpoint is removed from an ordering or bill paying process, nothing will trigger verification of a high-dollar purchase or invoice for payment. Therefore, before any process is streamlined, a careful mapping of the streamlined process should be developed and an analysis of any process change should be made in the context of what level of control is being eliminated. Any cost-cutting measure resulting in a reduction of the level of control has the potential of growing the opportunity side of the Fraud Triangle.

How interviewing can help to detect fraud

Combining the distinct skill sets of investigators and auditors is a best practice that will increase the chances of a successful fraud investigation and prosecution. Enhancing this collaboration is a skill that both groups possess—interviewing—which can be honed through further cooperation and refinement.

Interviewing, even in this age of technological advancement, is still the greatest weapon in the arsenal of the investigator and perhaps,

"Whenever there is a top-down initiative to reduce costs, efforts to streamline a process should be closely monitored because key controls may be eliminated...Any cost-cutting measure resulting in a reduction of the level of control has the potential of growing the opportunity side of the Fraud Triangle."

an underused asset of the auditor. Detecting potential deception and/or discomfort in the interview can provide an interviewer with a road map to areas of inquiry more likely to yield information relevant to an investigation. Although there are many methods and diverse opinion on the subject, the one thing universally held is that there is no such thing as an absolutely flawless method of detecting deception during an interview. Despite this limitation, it can be argued that, through a methodology and series of pointed interview questions, the interviewer should not strive to identify deception but work towards attaining the more manageable goal of identifying areas warranting further inquiry.

Fundamental to identifying possible deception or discomfort is assessing whether the interviewee appears to be simply providing information or attempting to manage the interviewer's perception. To aid in the comparison, consider the stereotypical image of a schoolteacher vs. the stereotypical image of a used car salesman. The more an interviewee's demeanor leans toward a schoolteacher, the more likely the information is truthful. Conversely, the more the interviewee's demeanor leans toward a used car salesman, the more likely the information may be deceptive.

It also may be helpful for the interviewer to develop a baseline of the verbal and nonverbal patterns of the interviewee's communication during nonthreatening dialogue. This baseline can then be compared to patterns observed

[14] Wikipedia, The Free Encyclopedia. Definition: "The tooth-tail" ratio is a military term that refers to the amount of military personnel ("tail") it takes to supply and support each combat soldier ("tooth"). March 1, 2015. (http://en.wikipedia.org/wiki/Tooth-to-tail_ratio)

immediately after specific lines of inquiry to identify departures from the baseline. Certain question types, such as open, closed, presumptive, indicator, and critical questions can also be employed to further ferret out discomfort or deception related to certain topics, individuals, or lines of inquiry. Important in this approach is the realization that one departure does not a deceiver make. In other words, the interviewee must look for a series of departures that are observed in response to a specific question[15]. Only then do the lines of inquiry meriting further investigative attention take shape. The use of such a practice, although not without limitations (e.g., cultural differences, unrelated stressors) can be a helpful means of maximizing time in an interview while uncovering relevant facts theretofore unknown.

FRAUD NEVER TAKES A VACATION: CASE STUDIES

When an individual's opportunity, need, and rationalization are blended with an organizational culture that embraces conceit, hypersensitivity, or obsessive cost cutting, it is likely that fraud is already prevalent or being planned. Think of prisoners confined to a maximum-security prison. It doesn't matter how escape-proof a prison may be, the inmates likely spend much of their waking hours looking for any vulnerability that they can exploit to escape. Similarly, people who handle cash probably spend at least a part of everyday fantasizing about how they could take some cash without being detected.

Of course, the vast majority of people are honest, have no overwhelming need to steal, and even report potential opportunities to commit fraud as vulnerabilities to be fixed. However, when fraudsters find opportunities to exploit, they use them as a means to steal to satisfy their cravings. The following examples are actual fraud cases where significant dollar values of material or cash were stolen. Only through the combined effort of auditors and law enforcement officers was the fraudulent activity discovered and the perpetrators brought to justice. Interestingly, both of these fraud cases occurred in organizations operating under a self-absorbed management culture of conceit, hypersensitivity, or obsessive cost cutting.

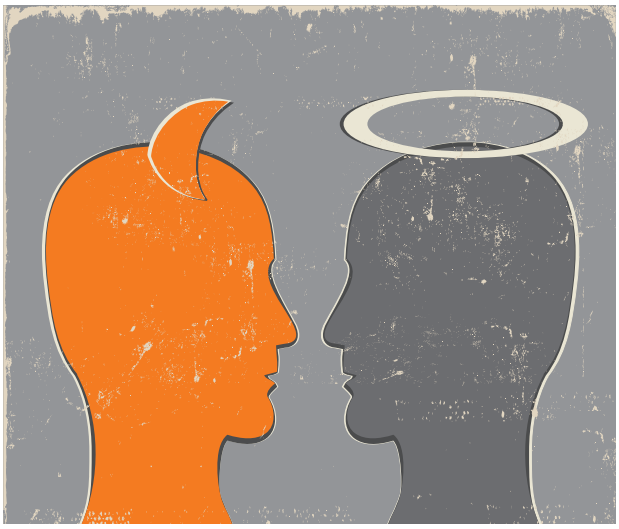
CASE STUDY 1: THE PURCHASING AGENT AND THE PURCHASING CARD

A female employee was issued a corporate purchase card to buy day-to-day items such as office supplies and make reservations for travel and meals. Her courteousness and helpfulness not only earned her a reputation of competence and dependability but also the trust of her supervisors, who granted her authority to not only make purchases, but to accept deliveries and authorize payments. As years passed, her reputation for efficiency continued to grow and her organization recognized her for being able to take on the responsibilities of three, ultimately reducing the number of people in the purchasing and receiving departments and saving money. As the volume of purchases continued to grow, the limits on the purchase amounts diminished and she was authorized to spend up to $100,000 a month without supervision.

One day, the purchasing agent's car broke down and she did not have the money or a personal credit card available to pay for the car repairs. She decided to borrow the company's purchase card to cover the unexpected cost and repay the $300 once she received her paycheck. When the purchase card bill came in with her $300 car repair on it, she realized that not only was the charge hidden among hundreds of other purchases but also that no one was likely to notice it since she was the only one reviewing the purchase card statements. As time went on, temptation got the better of her and she began buying gas for her car, personal meals, and some small gifts using the purchase card. As she predicted, no one ever noticed because she was still recognized as a trusted and dependable employee.

[15] Spy the Lie, Philip Houston, Michael Floyd, and Susan Carnicero, with Don Tenant, 2012, St. Martin's Press.

In fact, as management lavished more and more praise on her, she began to rationalize she was deserving of the one thing management did not provide to her—a pay raise. Through rationalization, she had no problem supplementing her lifestyle (need) through the company purchase card because—in her mind—she had earned it. As a few years went by, her company grew as did the volume of purchases. While management initially thought to hire an additional purchasing agent, she insisted that she could handle the added load so the hiring requisition was pulled. The management team thanked her for her dedication and hard work and at the same time reminded each other how adept they were at choosing extraordinary talent, such as their stand-out (and sole) purchasing agent.



The brazenness of the purchasing agent escalated because her lifestyle "needs" grew into an addiction for new cars, motorcycles, lavish vacations, and even cosmetic surgery. She was able to have it all bought and paid for by the company without anyone noticing because she kept up the appearance of being highly competent and trustworthy, which fed the egos of management. Everyone was happy—until the day the good times were brought to an end by a couple of sharp auditors.

Coincidentally, news reports began appearing about the emergence of corporate purchase card fraud. The gist of the reports was that the cost savings and paperwork reduction generated by relying on credit cards to streamline purchases also reduced internal controls over purchase authorization and order placement. The only way to ensure that credit card purchases were appropriate was to make sure that the time-honored tradition of separation of duties was in place.

While the conceited managers in this example were convinced that the purchasing agent would never commit fraud, the company executives disagreed. Because the credit card purchases had grown so large, the executives decided that independent assurance was needed and an audit was ordered.

The audit began and nothing was particularly noteworthy except for the large volume and diversity of items purchased. The auditors began digging through the transactions while also reviewing the corporate policies relative to prohibited vendors or merchandise. After a few days, the auditors noticed that airline tickets had been purchased from Southwest Airlines when the company had an agreement that all air travel would be purchased from United Airlines. If United Airlines could not meet the company requirements, a waiver from management authorizing a ticket purchase from another airline was required.

When asked, the purchasing agent said there was a waiver somewhere but she could not put her hands on it. The auditors continued their review and found more than a dozen airline tickets that were not associated with United Airlines. Then, the auditors went one step further and determined that the tickets were used by either the purchasing agent or someone who was not an employee of the company being audited. These dubious purchases only invited more scrutiny for all the remaining purchases. Suddenly,

the audit scope was expanded to include a review of every purchase made during the five years the purchasing agent was employed.

The results were staggering. By the time the detailed audit was mid-way, law enforcement had already joined the audit team to try to recover the merchandise purchased and to determine whether any vendors were paying kickbacks in return for receiving the purchase orders. When the audit and investigations were completed, more than $200,000 worth of merchandise was identified as being fraudulently purchased, including two automobiles, a motorcycle, four cruises, designer clothes and handbags, a wedding dress and reception, a variety of electronics and computers, and many other items.

The purchasing agent tried to gain the sympathy of the auditors and investigators by portraying herself as a victim who was subjected to such high levels of job-related stress that her only escape was retail therapy. She promised to cooperate and return as much of the merchandise as possible but said she had sold the electronics, the automobiles, and the motorcycle.

While she had indeed sold the automobiles, she lied about the motorcycle and most of the high-end electronics, which were hidden in her father's home in another state. After her conviction, she was sentenced to six to ten years in prison, and was required to make restitution. Her father and brother were convicted of receiving stolen merchandise and, while they escaped jail time, they were fined and placed on probation. The conceited cost-saving managers were terminated without consequence, except for earning a reputation for incompetence.

CASE STUDY 2: MILITARY SUPPLY CENTER "SURPLUS"

It would seem that in times of crisis or war our national goal to prevail would automatically override anyone's desire to commit fraud. Unfortunately, no matter how critical an asset is to supporting our men and women in uniform, there is always a civilian demand for military equipment. Once the shadowy realm of international arms dealers, the theft and sale of military equipment has been transformed by the Internet into a "Mom and Pop" operation.

In this scenario, the disproportionate focus on equipping the soldier (tooth) actually allowed acceptance of a streamlined control process (tail), resulting in a situation where the teeth ate the tail.

In 2013, an equipment vendor noticed merchandise for sale on eBay that matched the equipment his company had just sold to the military. While the eBay listing identified the equipment as "military surplus," the vendor knew the battlefield protective eyewear listed for sale was almost exclusively reserved for the military and was not surplus. The vendor reported his concerns to Defense Department investigators, who then began to monitor the eBay sales of the battlefield glasses and other items posted by the same seller on eBay. Their investigation led to an employee at a supply center for the military. By working undercover, the investigators determined that the items posted on eBay were most likely stolen from the supply center but the investigators had no way of knowing how many items were missing. Consequently, the investigators requested the support of forensic auditors to perform the accounting techniques necessary to determine which type and how much equipment was missing.

Because the protective glasses were the first item identified as stolen, the auditors began an examination of all orders for the special eyewear to determine how many pairs were purchased and then how many were issued to the troops deployed throughout the world. While tens of thousands were ordered, the auditors quickly determined that several thousand were missing after analyzing the glasses issued, the number ordered, and the number on hand. By reviewing the ordering forms, the auditors noticed the forms were often not signed or bore an illegible signature.

Next, the auditors looked at the shipping invoices to determine who accepted the eyewear for inventory into the supply center's warehouse and how the eyewear was eventually issued to the soldiers headed for the battlefields. Again, the records were often missing or illegible, forcing the auditors to rely on the vendor's records to determine how many glasses were ordered and who made acceptance on behalf of the military supply agency. By the end of their forensic review, the auditors were able to determine that more than 2,000 pairs of protective glasses could not be accounted for in the books and records.

The auditors then expanded their search to items specifically manufactured and designed for military uses that were also in demand throughout the world. By the time their review was completed, the auditors determined that there were as many as 20,000 items unaccounted for and valued at nearly $1.2 million. Another 11,000 items valued at nearly $1.2 million were purchased by the supply center and then labeled as excess and supposedly turned over "for disposal"—a term for many items that often turn up in surplus stores and eBay. Once the auditors' information was provided to investigators, search warrants were obtained and 2,500 stolen items were found in the home of one of the fraudsters operating an eBay account.

As part of a plea deal, the fraudster confirmed what the auditors found and identified his co-conspirators. He also acknowledged that the supply operation was hopelessly understaffed. He and his colleagues quickly realized they could order any amount of merchandise they wanted as they would always label the purchase order "urgent need." This automatically allowed the purchase request to be processed through an expedited, streamlined process where the "urgent need" status trumped all controls, including the standard separation of duties.

"Inadequate staffing created a control environment that was a contrivance of combined duties, shoddy to non-existent record keeping, and nonexistent internal audit/management reviews, providing many opportunities to commit fraud."

The fraudsters were also empowered to perform their own inventories and self-report on quantities ordered, issued, retained for on-hand inventories or identified as excess. Most importantly, the operation was highly regarded by local officials because the needed items were successfully reaching the soldiers on the battlefield (the teeth). Therefore, if the battlefield requirements were being met, then the supply center (the tail) was recognized for getting the job done. To the fraudsters, it could not get any better: they were commended for being able to get the job done efficiently with a small staff, while effectively supporting the soldiers in need.

The fraudsters were able to take advantage of a lax environment knowing their conceited leadership was far more focused on equipping the soldiers than worrying about internal controls. In this example, a disproportionate focus on equipping soldiers gave rise to a streamlined control process. Inadequate staffing created a control environment that was a contrivance of combined duties, shoddy to non-existent record keeping, and non-existent internal audit/management reviews, providing many opportunities to commit fraud. In the end, however, the fraudsters were convicted, sent to prison, and ordered to make restitution for the funds stolen.

CONCLUSION

LESSONS LEARNED

Auditors	Investigators
• Guided by standards	• Guided by the law
• Test internal controls	• Test if laws were broken
• Have access to records	• Can seize records
• Report missing inventory	• Recover stolen inventory
• Follow the money	• Capture the money
• Recommend controls	• Enforce the law
• Report security weaknesses	• Provide security

The ever-growing reliance on digital and electronic commerce to conduct business has increased the risk of fraud, waste, and abuse. The days of paper trails to follow the money and independently confirm the validity of transactions have been replaced with electronic records where the theft of money is much more difficult to trace. Today's moderately skilled fraudsters find ways to circumvent IT controls to commit fraud while simultaneously making fraudulent transactions appear valid. In our modern business environment, the controls once inherently provided by virtue of people working independently of each other have been replaced by easily exploitable digital processes—all in the name of efficiency. While auditors and investigators have increased their IT skills to meet the challenge of digital fraud, the added ingredient of teaming greatly strengthens the ability to fight fraud, waste, and abuse.

In the past, auditors could rely on paper trails and controls testing to identify weaknesses leading to missing inventory or cash. In fact, auditing standards rightly place hard copy documents as the most preferred evidence for supporting audit findings and opinions. Conversely, testimonial statements are considered by auditing standards as the weakest form of audit evidence. Fortunately, investigators have the credentials and authority to interview people under oath and use such statements as evidence in a court of law. While investigators often rely on "paper work" for evidence, they are not necessarily trained in forensic accounting to identify amounts of stolen or missing inventory. However, by collaborating and combining the skills of the audit and investigative professions, the battle against fraud, waste, and abuse can be more effectively fought.

ABOUT THE AUTHOR

Richard Leach, CIA, CFE, Director and Senior Advisor

Richard (Dick) Leach, CIA, CFE, is a Director and Senior Advisor with CohnReznick's Government and Public Sector Advisory Practice. Dick joined CohnReznick from the U.S. Navy, where he served as the Auditor General for 14 years and was a member of the Navy Senior Executive Service for more than 25 years. During his tenure as Auditor General, he served as the Department of Defense representative on the Comptroller General's "Yellow Book Committee," Chair of the Defense Contract Auditing Agency Oversight Committee, and Chair of the Audit Committee of the Defense Finance and Accounting Service. Dick also designed and oversaw the implementation of the internal control and audit plan for two rounds of Navy and Marine Corps Base Closure and Realignment Processes. He is a member of the Association of Government Accountants (AGA), the American Society of Military Comptrollers (ASMC), the Institute of Internal Auditors (IIA) and the Association of Certified Fraud Examiners (ACFE), the Veterans of Foreign Wars (VFW), and the American Legion.

GAIN INSIGHT

Including CohnReznick as part of your potential fraud risk exposure will provide you with access to deep industry and government knowledge, insight, and expertise.

For more information on how to implement or perform a fraud risk assessment, please contact:

Frank Banda, CPA, CFE, CGMA, PMA
Managing Partner-Public Sector, CohnReznick
301.280.1856
frank.banda@cohnreznick.com.

ABOUT COHNREZNICK

As a leading advisory, assurance, and tax firm, CohnReznick helps forward-thinking organizations achieve their vision by optimizing performance, maximizing value, and managing risk. Clients benefit from the right team with the right capabilities; proven processes customized to their individual needs; and leaders with vital industry knowledge and relationships. Headquartered in New York, NY with offices nationwide, the firm serves organizations around the world through its global subsidiaries and membership in Nexia International. For more information, visit www.cohnreznick.com.

1301 Avenue of the Americas
New York, NY 10019
212.297.0400

cohnreznick.com

CohnReznick
ADVISORY • ASSURANCE • TAX