WILL I GET CAUGHT?

SPEAKING TO THE MIND OF THE PERPETRATOR: A NEW FOCUS FOR INTERNAL FRAUD PREVENTION

By Steve Dawson, CPA, CFE

"If I thought they were looking, I never would have done it." In my 35 years of conducting internal fraud investigations, this is one of the most common statements I hear from guilty parties after we obtain a confession.

Performing investigations day in and day out, my desire is to learn from each of these confession-seeking interviews. I want to understand what could be done to prevent fraud from happening in the first place. Could the company design better controls? Dual authorizations? Signature thresholds? Segregation of duties? I get plenty of ideas from these investigation post-mortems.

Creative new schemes inspire creative new tactics to discourage fraud. Yet even with newer and more specific control activities, I never seem to complete an investigation before five more are waiting around the corner. I constantly ask myself: "What am I missing? What more can I do to help organizations prevent internal fraud?" I have to conclude that all of these controls just don't seem to be working.

Back to this revelation from guilty parties, "I never would have done it IF..." The possible answer appears and the light comes on for the first time. A stronger strategy is right in front of me and really always has been. "I never would have done it if I THOUGHT they were looking." Not "if I KNEW" but rather "if I THOUGHT."

Thinking an organization is watching is what the Association of Certified Fraud Examiners refers to as the "perception of detection." The ACFE states that this perception of detection is the number one internal control that can be implemented to prevent internal fraud. Regardless of the size or complexity of a business, this preemptive environment of discovery is one of the most successful ways to deter internal fraud.

It's clear that we need this new focus, this new approach to internal fraud prevention. We must address the mind of the potential perpetrator, his/her thought process and how to increase this perception of detection.

The Potential Perpetrator's Thought Process

Stage 1: Need/Greed – Due to financial pressures, individuals encounter financial needs that must be addressed. If a critical need is not present, often greed is the motivator. Regardless of need or greed, once the idea to commit a fraud is born, the potential perpetrator moves into Stage 2.

Stage 2: Will I Get Caught? – Potential perpetrators weigh the chances of getting away with the scheme. If they believe that they can follow through with their plan undetected, they approach Stage 3.

Stage 3: The Wall of Internal Controls – Historically, this is where we invest our time in fraud prevention. We focus on building a wall of control activities, adding this control and that control, until we believe we have a barrier so tall no one can scale its height. Often, we build controls from previous experience with fraud or examples we've seen elsewhere. The controls are built after the crime has already occurred. The trouble is the next potential perpetrator simply evaluates this wall of internal controls, sees where people are watching for fraud (or even recognizes that no one is truly looking at compliance with the controls), walks calmly around the wall, circumventing its effectiveness, and we have a new fraud to investigate.

Figure 1: Stages of a Perpetrator's Thought Process

The three stages of a potential perpetrator's thought process include:

- **Stage 1:** Need/Greed
- **Stage 2:** Will I Get Caught?
- **Stage 3:** Circumventing the Wall of Internal Controls

While control activities are important, what if we shifted our focus from building Stage 3 barriers where people are already creating ways to commit fraud and already planning how to get around the wall of internal controls? Instead, we speak directly to the mind of the potential perpetrator. We interrupt their thought process in Stage 2 where they are considering their potential to be discovered. We seek to effectively stop the development of the scheme itself by answering the question "Will I get caught?" with a resounding YES.

The Perception of Detection

What can we implement that stops a potential perpetrator in Stage 2? We use simple processes and procedures, typically less expensive to implement than full control activities. These processes increase the perception of detection, not the probability of detection or the possibility of detection, but the perception of detection. We address the statement, "If I thought they were looking ..."

In my investigation practice, I drive the highways of this country often. On one highway in particular, I drive through a small town that always has a sheriff's patrol car parked in the bar ditch parallel to the highway. As I approach the area, seeing the patrol car, I do what every other driver does; I make sure I drive the speed limit, obeying the law. As I pass, I glance into the windows of the patrol car and notice that no one is actually in the car. In effect, this car can do nothing to catch and penalize me for speeding through town. But did I speed through town? No, and neither does anyone else. No one wants to chance getting a ticket.

The presence of the car increased my perception of detection; I changed my behavior realizing I could get caught speeding. Even residents of this town familiar with the empty car know there is a chance someone could be there next time. It's just not worth getting the ticket.

How can we apply this type of technique to internal fraud prevention? Let me insert myself into the shoes of a perpetrator. I am an employee performing a shell company fraud. I commit the crime by creating fictitious invoices for my employer; my employer pays the shell company that I own. No one knows I own this shell company. It just looks like a normal supplier.

One day, my supervisor comes to my office with a Conflict of Interest Form. She explains this is a new form that all employees are now required to complete on an annual basis as part of our new periodic master vendor file review. I am asked to disclose any companies that we do business with where I may have a conflict of interest, such as ownership, personal relationships, family relationships, etc. Am I going to disclose my shell company on this form? Of course not. It's a fraud. My employer will not actually gain any useful information and it seems as though this whole new vendor review process is worthless in detecting my scheme.

But what is achieved is heightening the perception of detection. I am now feeling very uneasy understanding

that my employer is looking more closely at vendors. I know I must complete this form annually and it's a part of a larger compliance process reviewing the master vendor list. I am now worried about other checks they are performing on vendors. What else are they asking and looking for?

Now, because of this new form, my perception of detection has increased exponentially. This one piece of paper, this empty patrol car, has created fear, regret and anxiety in my fraudster's conscience. If I had this information before I created the shell company, if I thought they were looking, I never would have done it.

This simple form is an example of a process focused solely on increasing the perception of detection, speaking to the mind of the potential perpetrator during the Stage 2 evolution of the fraud thought process. This form and other processes like it cost pennies to produce.

Increasing Awareness

So how do you begin? As part of this new focus of prevention, I believe you can significantly raise the perception of detection in your workplace by implementing or strengthening processes in the following areas:

- Education,
- Targeted control processes,
- Effective fraud reporting,
- Modeling of ethical leadership, and
- Other physical controls.

Education

Educating the workforce increases fraud awareness. This does not have to be overly time-consuming. Most organizations already conduct periodic company-wide staff meetings covering many different operational areas. Consider adding 15 minutes to each meeting and address issues such as the definition of internal fraud or the costs of fraud.

Defining fraud (schemes, theft against the organization by its own officers, directors and employees, attacks from within, betrayals of trust, etc.) helps identify issues the company is already protecting against. Talking about the costs – fewer pay increases, increased layoffs, decreases in employee benefits, low employee morale, legal fees and investigation costs – requires all employees to consider specific consequences and encourages them to want to deter fraud, as well.

These meetings could review the existing policy or how to report suspicious activity. The point isn't to create experts in prevention. However, every time fraud is mentioned or discussed as a subject in a staff meeting, the workforce understands that the company is proactive in preventing it. They hear that the topic is important enough to discuss with everyone.

Companies should perform periodic risk assessments to determine those areas most vulnerable to fraud.

Targeted Control Processes

All companies should perform periodic risk assessments to determine the most vulnerable areas. I recommend seeking the input of various employees, regardless of rank or tenure. If an employee provides input into the risk assessment process and the design of internal controls to address those risks, I believe that he/she will be less likely to steal from that process.

Those organizations that have an internal audit function should communicate the content of the audit workplan to the workforce periodically. This makes employees aware of the areas that may be looked at for fraud.

Organizations should revisit older control processes that have been abandoned over time. Some of these age-old processes are honestly some of the most effective controls I have seen, such as:

- Mandatory consecutive vacation days,
- Rewards for whistleblowers,
- Surprise audits (such as cash counts),
- Job rotation/cross-training.

While these controls can be considered typical of the Stage 3 Wall, their power in this new focus is about communication. Communicating that controls exist makes a potential perpetrator think twice if he/she understands a vacation, surprise audit or job rotation could reveal his/her fraud.

Effective Fraud Reporting

Every organization should have a fraud policy/reporting policy as part of a strong anti-fraud program. The policy should include enough information defining fraud and explain typical warning signs. It should put the potential

reporters at ease, letting them know they don't have to be experts and that they have certain whistleblower protections. The workforce needs a mechanism to report their suspicions. Most reporting mechanisms are structured anonymously and can be either internally or externally administered.

Most importantly, the existence of a reporting mechanism should be continually communicated to the workforce. Communication raises awareness, which raises the perception of detection.

Modeling of Ethical Leadership

Roman Emperor Marcus Aurelius once said, "A man should be upright, not kept upright." It's a beautiful thought. Unfortunately, assuming every person lives up to this ideal is not practical.

In his book *Why People Obey the Law*, Tom R. Tyler points out that historically, a workforce will adopt the same ethical mindset as its leaders. He outlines the Principle of Legitimacy, which states that individuals will obey the law based on their perception of, or belief in, their leaders.

A workforce will adopt the same ethical mindset as its leaders.

Accordingly, company policies should reflect standards expected of all individuals and should be modeled first by company leadership. Organizations should develop foundational policies that include the following:

- **Code of Ethics** – The content should address various areas, such as the use of common sense in making ethical decisions, competition, conflicts of interest, gifts from outside the company, outside employment and the proper treatment of confidential information.

- **Fraud Policy and Reporting/Whistleblower Protection** – A fraud policy is an absolute necessity. Its content outlines the measures that will be taken in the event of a suspected fraud. The policy itself provides information that educates the workforce, thus raising the level of awareness. The provisions that address reporting and whistleblower protections provide a framework for how to handle suspicions correctly, thus protecting the workforce, as well as the company.

- **Policy Provisions that Remove an Employee's Presumption of Privacy** – These provisions address the fact that the company provides employees with the tools necessary to perform their job functions (computer, email, mobile phone, tablet, desk, office space, vehicle, etc.) and that these items have no presumption of privacy associated with them. The provisions state that all company-provided items are subject to search with reasonable probable cause.

Company leadership can model ethical responsibility by committing to periodic updates or reviews with the workforce, adherence to the standards themselves and consistent handling of fraud suspicions in accordance with these policies. As with any company policy, all policies should be developed in conjunction with company legal counsel.

Communicating these policies on a regular basis raises the level of overall fraud awareness. A potential perpetrator knows what is expected, knows what policy provisions are in place, knows that all other coworkers are aware of this information and can effectively answer the Stage 2 question, "Yes, I probably will get caught."

Other Physical Controls

We rarely enter an establishment that doesn't have some type of security system. The system usually includes the bubble lens cameras used to monitor customer and employee activity. This is a physical, visual control that lets an employee know that he/she could be seen performing some type of nefarious act.

Previously, I stated my recommendations for increasing the perception of detection were inexpensive. If a complete bubble lens security system is not immediately fiscally possible, consider a dummy bubble (think empty patrol car). It still contributes as a deterrent, as it creates an environment of watchfulness.

Physical controls can also include various analytical software that monitors email and internet usage. The programs can perform text analytics like text categorization, text clustering, sentiment analysis, lexical analysis, etc. The descriptions and applications of these programs can certainly go far beyond Stage 2 intervention. But simply having them and communicating the organization's access to them, is a control in and of itself. If a potential perpetrator knows his/her email and internet usage might be monitored, he/she will understand the chances of getting caught rise exponentially.

Keys to Preventing Fraud

Whether controls are fully established or still developing, if they are perceived to exist, the perception of detection has increased and internal fraud can be prevented. Through education, targeted control processes, effective reporting, the modeling of ethical leadership and the existence of other physical controls, I believe companies can efficiently implement processes that serve to raise the level of fraud awareness.

Without abandoning the Stage 3 Wall of Internal Controls that should be under constant construction, we can attempt to interrupt potential perpetrators earlier in their thought process. We can give them ample evidence to conclude "Yes, I will get caught" when considering a scheme.

The ideal is an environment where no employee is bold enough to step up to the Stage 3 Wall. Instead, if the financial need is great enough, the desired result is an employee who finds another way to handle life's struggles by seeking help, and remaining a productive, valued employee and person.

ABOUT THE AUTHOR:
Steve Dawson, CPA, CFE, is the President of the Dawson Forensic Group and for over 30 years, has performed forensic investigations, internal fraud prevention consultations, accounting records reconstruction, litigation support services and forensic training services. His book *Internal Control/Anti-Fraud Program Design for the Small Business* is available through Wiley Business Publishing.

For more information, visit his company website www.dawsonforensicgroup.com or email him at steve@dawsonforensics.com.