CHANGING REGULATORY REGIME NECESSITATES NEW SOLUTIONS TO AN OLD PROBLEM:

5 ELEMENTS CRITICAL TO AN ANTI-FRAUD COMPLIANCE PROGRAM

US government regulators have become more aggressive in their detection and enforcement of fraud against the government. One of the key tools they are using to combat such fraud is the False Claims Act. Most FCA cases are filed under the act's qui tam provisions, which allow whistleblowers (relators) to bring a private action on behalf of the government.

Due to changes in the regulatory regime, whistleblower lawsuits have become even more attractive to employees (and even competitors), who stand to gain payouts of 15 percent to 30 percent of the total recovery. In the first half of 2014 alone, the government has used the FCA to recover more than $2 billion.

FCA cases have been brought against individuals, companies, universities and nonprofit charities in various industries. More importantly, **FCA cases have been brought under a wide array of theories,** including fraudulent billing practices, false compliance certifications, import/export duties violations, provision of inferior goods, government grant fraud, failure to follow Current Good Manufacturing Practices, failure to pay royalties, fraudulent mortgage and underwriting practices, fraudulently reimbursements, fraudulent practices relating to government service contracts and failure to return overpayments.

OLD PROBLEM, NEW RISKS

While fraud has always been a problem affecting both the functioning and bottom line of businesses, the FCA has converted this business problem into a serious legal risk. With penalty provisions awarding treble damages and statutory fines, as well as the risk of suspension and debarment, the costs of letting fraud involving the government go unchecked can be significant. Businesses need to be proactive and evaluate their existing compliance and controls to make sure they are detecting fraud in the workplace.

FRAUD IS A COMPANY'S "MOONWALKING BEAR"

Although companies endeavor to prevent fraud, this goal is one of several, easily distracting obligations central to the business. An organization's responsibility for detecting fraud in the midst of these competing obligations is akin to the responsibility for detecting a moonwalking bear – the central concept of a popular awareness test commercial aired on British television. At the commercial's outset, viewers are given 16 seconds to count the number of ball passes made by a white-clad basketball team as two teams race around the court and between each other tossing balls among their teams. Viewers typically concentrate on the task of counting the passes. But the test's true question, revealed at the end, is: did you see the moonwalking bear? Most viewers say no. Yet when the clip is replayed, it becomes clear that during the test a tall black grizzly bear walks to center court, then moonwalks off – utterly unnoticed by most viewers, whose attention is wholly on the ball.

FINANCIAL STATEMENT AUDITS ARE NOT THE SOLUTION

Financial statement audits are not the solution and cannot be relied upon to uncover FCA fraud. Indeed, companies that uncover fraud are often surprised to learn that it escaped detection by the financial statement audit. Yet, internal audits only detect about 14 percent of occupational fraud and external financial statement audits only detect about 3 percent of occupational fraud.

What accounts for these percentages? The following are reasons why financial statement audits may fail to detect fraud.

1. Audits are limited in scope. Financial statement audits are limited in scope and concern the reliability of financial statements and, in certain instances, internal controls over financial reporting. The task of a financial statement audit is not to ferret out FCA violations and given that a FCA violation does not necessarily link to a financial misstatement, it is not expected that a financial statement audit will uncover a FCA fraud.

2. Fraud is hidden. Fraud is a crime where the perpetrator endeavors to conceal unlawful activity and to mislead others about what is really going on. Perpetrators have fabricated a scheme with a ***believable yet fake concealment narrative,*** often substantiated with fake documents to conceal their activities ***and evade the presence of controls.***

3 Audits use sampling. Auditors do not examine every transaction or event that occurs in a company's fiscal year. Furthermore, the auditor's focus on materiality requires the auditor to make judgments on which data to assess. Perpetrators often target smaller accounts that are not material to financial statements and are likely to be outside the purview of an audit. It is just as often the case that the actual transaction is accounted for correctly, even if it violates the FCA. Consequently, FCA fraud will typically remain concealed despite a thorough audit.

4. Auditors are not police investigators. Nor are they document authentication specialists or criminal lawyers. Thus, skills relevant to a fraud examination, such as ensuring that a document is not fabricated or obtaining an admission to a crime, are ***not necessarily*** within an auditor's skill set. Given the complexity of fraud, and the fact that this type of fraud is typically not aimed at manipulating financial statements, the likelihood that financial statement auditors will "naturally" discover FCA fraud in the ordinary course of an audit is extremely low. Indeed, the percentage of frauds found by external audit (only 3 percent) is significantly less that the percentage of frauds detected by ***accident*** (6.8 percent).

5. Insiders have the ability to override controls. The American Institute of Certified Public Accountants (AICPA) has deemed management override of controls the "Achilles heel of fraud prevention." Often times, the very people within organizations who design, implement and maintain internal controls can also override and bypass them – and in such cases, detecting fraud is even more difficult. These individuals are often at senior levels, including management or higher ups, and are part of the reason that financial losses to an organization increase with the perpetrator's seniority. For instance, there is a median loss of $500,000 when a perpetrator is an owner or executive, as compared to a median loss of $130,000 when the perpetrator is a manager and a median loss of $75,000 when the perpetrator is an employee. Thus, even if the FCA fraud does not have a direct and material impact on the financial statements, the perpetrator is often in a position to override the controls otherwise relied upon to produce accurate financial results.

6. Audits are not designed to uncover crimes that do not necessarily impact the financial statements. Although auditors are required to employ professional skepticism, the traditional audit is non-adversarial. Yet, perpetrators are by definition attempting to conceal a crime and will always have a noncriminal justification for their actions. To get underneath that justification and ascertain whether the suspected perpetrator has *scienter*, or an intent to knowingly engage in a wrong act, may require interviewing individuals. These interviews may require a more probing tone and a variety of important legal considerations that do not fall within the purview of a traditional audit and that necessitate direction of counsel.

7. Auditing is distinct from a fraud examination. Fraud examinations attempt to mitigate the blind spots of audits by moving fraud to the forefront of an examiner's detection. Unlike audits, fraud examinations are not regularly scheduled, but are conducted consistent with business needs and sufficient planning. Also, fraud examiners perform an investigation to determine whether specific allegations of fraud can be substantiated and, if so, what gaps or weaknesses exist within specific anti-fraud controls. Given the presence of a fraud allegation and a potential perpetrator, examinations can be more probing and adversarial than an audit. Finally, fraud examinations include the direction and counsel of an attorney, due to the potential that a crime may have occurred and the need for privilege.

A NEW SOLUTION FOR NEW RISKS

For organizations to stay ahead of occupational fraud and its legal, reputational and financial consequences, responsibility for detection cannot be solely on the auditors – it must be shared. The five elements below are critical to a successful anti-fraud compliance program.

1. Collaborate across your organization.

Fraud is often collusive. The largest fraud schemes (a median average of $550,000) were committed by four or more persons. This is due to a group's ability to subvert a broader range of the checks and balances that might otherwise detect fraud. Due to the collusive nature of large frauds, preventing and detecting fraud cannot be a one-man or -woman show. A collaborative approach with the support of legal, audit, IT, loss prevention, human resources, management and the board, who are committed to preventing fraud in their roles within the organization and to working with other departments, will help ensure that established controls are not overridden by a siloed approach to prevention.

2. Take advantage of insider knowledge: use employee hotlines.

Employees are an organization's first line of defense against fraud. Approximately 40 percent of frauds are uncovered as a result of tips. The majority of tips come from employees. Tips are twice as effective at fraud detection than management reviews, audits, account reconciliation, document examination, surveillance and monitoring, law enforcement and IT controls. Organizations should take advantage of this insider knowledge and employ hotlines to learn from their employees about the potential fraud they are seeing. Organizations with hotlines have better fraud detection results in all of their anti-fraud controls than do organizations without hotlines.

3. Make your people "fraud aware" at every level.

Reduce the risk of nuisance reports by ensuring that the organization's personnel are fraud aware and are clear on what does and does not constitute suspicious behavior. Given that fraud losses occur at every level of an organization (more costly at the top, more frequently at the bottom), anti-fraud training should be mandatory for all personnel – not only auditors – on fraud risk factors, consequences for the individual and the company, the company policy on fraud, and common behaviors that create control weaknesses and allow fraud to take root. Training should be specific to how fraud can occur in their business lines and role and should be tested both immediately after training and periodically to ensure employees have internalized the training's teachings. This will allow organizations to instill fraud awareness through their tone at the top, mood in the middle and buzz on the bottom.

4. Put in place fraud-specific controls.

Because fraud presents a challenge of uncovering a crime hidden due to the appearance of compliance, policies and controls specific to rooting out fraud are necessary to prevent fraud and ensure it is not lost among competing compliance priorities. Organizations without fraud controls should consult with legal counsel or an investigator specializing in fraud to find out the menu of available options and strategize on what will work best. Data is now available on the effectiveness of various anti-fraud controls, including what are the most common, the most effective, most frequently used and biggest value controls. Organizations that already have fraud controls and would like to get a better handle on how to engage in fraud prevention – whether before or after an incident – should retain outside counsel and/or an investigator specializing in fraud to help them assess weaknesses in their anti-fraud program, design improved policies controls and educational tools and test these improvements against their workplace.

5. Don't just monitor – stay up to date.

As renowned management consultant Peter Drucker has said, "What gets measured gets done." Organizations may already have compliance programs, but if they do not periodically evaluate and update their anti-fraud controls, the confidence they have in their program lacks basis. Perpetrators are always seeking innovative ways to carry out their designs. For companies, routinely testing controls and updating systems is essential. Representatives from in-house counsel, compliance, audit, human resources and IT should undergo periodic training with counsel and/or investigators, who specialize in fraud, to keep them abreast of the latest fraud schemes, prevention methods and consequences of fraud within their organizations so that they may be anti-fraud leaders in their workforce.

ABOUT US

DLA Piper is a global law firm with lawyers across the Americas, Asia Pacific, Europe and the Middle East.

From the quality of our legal advice and business insight to the efficiency of our legal teams, we believe that when it comes to the way we serve and interact with our clients, everything matters.

FOR MORE INFORMATION

To learn more about DLA Piper, visit www.dlapiper.com or contact:

Savaria Harris
Partner
savaria.harris@dlapiper.com
New York
T +1 212 335 4553

Savaria Harris is an experienced litigator with trials in state and federal courts as well as with government and internal investigations in the white collar context.

Her practice centers on providing clients with an integrated approach to addressing fraud, whistleblower and government actions under the False Claims Act and its local equivalents. She is experienced in risk assessments, internal investigations, ethics and compliance training, as well as litigation and trial representation. In addition to her practice, Savaria is an adjunct professor of Workplace Ethics at Georgetown University, a member of the Advisory Council for the Association of Certified Fraud Examiners and a member of the NYU Program on Corporate Compliance and Enforcement.

www.dlapiper.com