Compliance & Ethics PROFESSIONAL

Vol. 8 / No. 4
08 / 2011

TOP STORIES INSIDE

Meet

Fernando M. Caleiro Palma

Anti-Corruption Program Manager for Archer-Daniels-Midland Company in São Paulo, Brazil

Society of Corporate Compliance and Ethics

7 Steps to Investigate Alleged Employee Misconduct

–Now including: *Writing Comprehensive Investigative Reports!*

2011

Seminar Series

Join us for our highly interactive, step-by-step seminar to learn practical skills for how to investigate and document allegations of compliance violations, fraud, harassment, discrimination, theft and other employee misconduct.

For details, visit:
www.globalcompliance.com/seminar

Course Overview

You are assigned to conduct an internal investigation. The facts are unclear and you are not sure who is telling the truth—yet you must reach a conclusion. In this hands-on seminar, you will learn practical skills for investigating alleged misconduct and ways to balance the rights of the complainant and the accused while protecting the interests of your organization. Plus, you will learn how to minimize administrative burden while writing effective investigative reports.

In this two-day workshop, you will learn:

- How to strategically investigate "he said/she said" allegations where there are no eyewitnesses
- How to interview witnesses using a specific method that enables you to gather all relevant information
- How the laws have changed regarding investigations (e.g.—is it lawful to use social media in your investigation?)
- Techniques and questioning strategies you can use to determine whether a witness is lying
- The rules for searching an employee's workspace, computer or personal belongings
- The appropriate standard of proof for imposing discipline
- What to include and not include in the report
- How to properly document credibility determinations and compile exhibits
- Privilege and confidentiality designations and who should see the report
- What documents to retain in the investigative file

Continuing Education Credit

Applications have been filed with the Society of Corporate Compliance and Ethics (SCCE) for the in-person sessions*, the 7 Steps Webinar has been approved for 6.9 units and the Report Writing Webinar has been approved for 3.3 continuing education units toward Certified Compliance and Ethics Professional (CCEP) credit. Multiple state bar associations have approved our Investigation and Report Writing Seminar for Continuing Legal Education (CLE) credit.

**Our website will be updated when approval is received*

2011 Dates and Locations

May 4–5	New York
May 11–12	Washington, DC
June 1–2	Chicago
June 9–10	Atlanta
June 15–16	Hartford, CT
September 21–22	Houston
October 5–6	Chicago
October 12–13	Dallas
October 19–20	New York
November 2–3	Los Angeles

Webinars

For the webinars, the Investigations and Reporting Writing classes will be offered separately.

May 18–19:	7 Steps to Investigate Alleged Employee Misconduct
May 25:	Writing Comprehensive Investigative Reports
October 26–27:	7 Steps to Investigate Alleged Employee Misconduct
November 1:	Writing Comprehensive Investigative Reports
December 7–8:	7 Steps to Investigate Alleged Employee Misconduct
December 14:	Writing Comprehensive Investigative Reports

View a detailed course outline, watch a video clip of the seminar, or register at www.globalcompliance.com/seminar

Phone: 800-443-9037 ▪ E-mail: seminars@globalcompliance.com

GLOBAL COMPLIANCE℠
Good for Business.

Contents

AUGUST 2010

Compliance is all about PEOPLE

By Daniel A. Cotter, JD, CPA

Much is made of corporate compliance programs. We hear the words "tone from the top" spoken often, referring to the top of a corporate entity. The Federal Sentencing Guidelines (the Guidelines) also refer to mitigation of fines, penalties, and sentencing for corporate bodies that have implemented strong compliance programs. Alexander Pope said "To err is human; to forgive, divine." As the quote notes, erring is a human condition. Statements such as "Mistakes were made" have been around since at least the 1980s, but we must be cognizant that, at the end of the day, an effective corporate compliance program is not about some lifeless corporation or other entity; rather, it is about the people. This article addresses the elements of an effective corporate compliance program—the acronym, PEOPLE.

PEOPLE is an acronym used in the statement "Compliance is all about PEOPLE." At a recent advisory board meeting for Wolters Klewer Financial Services Products, each compliance officer was asked to explain to his or her boss what elements they thought should be contained in a compliance program. With that task at hand, the following six compliance elements were, in one way or another, expressed by all of the attendees:

- Policies and procedures
- Education of employee base
- Operations implements changes
- Process of review and revision
- Legal/Audit/Compliance/Operations/IT
- Evaluation of the overall compliance program

The first letter of each of the bullets, taken together, spells PEOPLE. The following sections address each of these elements in a little additional detail.

Policies and procedures

It all begins with this step. Without policies and procedures that can set the "tone at the top" and guide your employees throughout your organization, compliance is an impossible task to master. Development of the appropriate policies and procedures is the starting point for an effective compliance program. The policies and procedures required will depend on the industry in which a company operates, but there are some standards that must be in any fully developed compliance program. These "must haves" include:

- Standards of conduct
- Conflicts of interest
- Antitrust considerations
- Privacy
- Sarbanes-Oxley Act of 2002 (if publicly traded)
- Insider trading (if publicly traded)
- Taxation
- Record retention
- Human resources
- IT security and safety

Many of these are contained in the employee handbook, but they could be found elsewhere. Once the policies are developed and in writing, dissemination is critical. Employees must have easy access to the policies and procedures, whether online or in hard copy, so that they can review the policies and procedures and acknowledge receiving them and reading them.

Education of employees

Dissemination is key to an effective compliance program, but it is not enough. The company must educate its employees. The Guidelines call for a training program that is commensurate with the size and complexity of the company. The more intimate the training, the better. A best practice is to hold the training in small groups and in person to make sure employees are paying attention and can have their questions addressed.

Training once and then forgetting about it is not a good practice. Rather, the training must be continuous. Annual training, at a minimum, on various policies and procedures is recommended. When employees join the company, part of the orientation process should be compliance—why it matters to the company, why it is the right thing to do, and how seriously the company and its senior management take compliance. It is not just the right thing to do; it is good business.

Operations implements changes

A Compliance department or chief compliance officer (CCO) is responsible for the overall compliance program. Sometimes other groups are involved. No matter how good the CCO or Compliance department is, at the end of the day, only those in Operations can effectively ensure that compliance is being implemented. With all of the changes that occur on a regular basis at the local, state, and national (and international) levels, best practice is to have some means of checking or verifying that the requirements of the compliance program are being done, and done correctly. Operations implements compliance and its myriad changes; compliance checks to ensure that things are being done correctly. Bottom line, "trust, but verify."

Process of review and revision

A compliance program cannot be stagnate. With all of the changes constantly afoot, the Compliance department should review the compliance program to determine what policies and procedures should be changed in light of experience or legal changes. When the review process calls for revisions to part or all of the program, it is imperative that the Compliance department or CCO go back to Step One, drafting and developing the policies and procedures, then progress through the remaining steps of PEOPLE.

Legal/Compliance/Audit/HR/IT/Operations

Everyone must work together. Policies and procedures can be developed and disseminated; however, this cannot be done in a vacuum without understanding the needs, constraints, and capabilities of other groups in the organization. One of the groups that is often left out of compliance discussions until late in the process is IT. In most instances, this is a fatal mistake. IT has a set budget and projects for the year. If a huge compliance revision needs to be made, almost certainly it will include revisions to IT systems. At some point in the process, all of the stakeholders in an effective compliance program must be at the table; my perspective is, the sooner the better. This will ensure a smoother path to an effective compliance program.

Evaluation of the overall compliance program

This final step, like the others, is a continuous one. How does one evaluate the effectiveness of a compliance program? One measurement is how many fines, penalties, citations, or other indications of violations have occurred during a given period. One measure might be how many calls have made it to the compliance hotline. Although these measurements will give a quantitative view of how things are progressing, don't lose sight of the qualitative measurements. How is employee morale? What reputation does the company have for being a good corporate citizen? What is the tone at the top, and is it rhetoric or reality?

With both the quantitative and qualitative information, you will have a sense of how well your compliance program is working for your organization. Armed with that data, you can then start at the top and go through the elements again. The work is never finished; it is a constant work in progress.

Conclusion

PEOPLE are the only things that make a compliance program work and an effective one at that. By keeping the PEOPLE elements in mind, you will be well on your way to ensuring that you

CONTINUED ON PAGE 9

Anti-corruption initiatives intensify: Does your training program measure up?

By Chanin Ballance

By now, it should be compellingly clear that the Foreign Corrupt Practices Act (FCPA) is no longer just a piece of paper floating around. The fines by the US government can be too severe to write off as a cost of doing business, and now we know that some prominent executives are going to prison—and it's not necessarily because of what they've done, but under the standard of willful ignorance—because of what they should have known others in their organization were doing.

No matter how you look at it, violating the FCPA can have a devastating reputational and financial impact on your organization. Therefore, your employees, vendors, contractors, and other third parties that you work with must clearly understand the laws and how to follow them. One efficient and cost-effective approach to solving compliance challenges is through online training.

Important elements for anti-corruption training

1. Tone from the top. As we know, an organization's leadership creates the tone. Setting the highest ethical standards is critical. Leaders and employees throughout the organization need to hear the message and hear it consistently. It is important for leaders to talk about the values of the company and to live up to those values.

2. Policies and procedures. Written policies and procedures form the cornerstone for any anti-corruption and anti-bribery program. Care should be taken that it be written in plain English and not "by lawyers for lawyers."

3. Enforcement. Internal company enforcement is essential, including ongoing monitoring, auditing, and assessment, but also granularity down to the individual employee level. There should be both "a carrot and a stick" so that employees are disciplined for compliance failures, but also rewarded—and seen to be rewarded—for doing business through appropriate compliance avenues.

4. Reporting and response. Under the FCPA, an anonymous reporting hotline should be a component of a company's overall compliance program. The UK Bribery Act calls it a "speak up"

CHANIN BALLANCE

line, but whatever it is called, there should be recognized reporting mechanisms in place that allow an employee to report allegations of bribery and corruption, and protections in place to guard against retaliation for such reporting.

5. Third-party compliance. Anti-bribery and anti-corruption programs discuss the risk of doing business with third parties. They all agree that this risk must be properly evaluated, investigated, and managed going forward. Appropriate due diligence must be performed, and compliance terms and conditions are important with all third parties. General oversight after the contract is signed is also a key element.

6. Record keeping and internal controls. Both the FCPA and the UK Bribery Act have language that makes clear that not only must books and records adequately reflect a company's expenses, but that internal controls are key defense and preventative measures against bribery and corruption.

7. Training. Training company employees with an annual certification is an important part of an effective anti-bribery and anti-corruption program. The UK Bribery Act extends this training to third parties.

Why train on this subject?

Laws such as the Foreign Corrupt Practices Act, the Lily Ledbetter Fair Pay Act, recent changes to the Health Insurance Portability and Accountability Act/Privacy and Security Rules (HIPAA/PHI) and many others are driving the need for increased and more immediate company compliance. US organizations spent $125.88 billion on employee training and development in 2009. Approximately $27.1 billion of that was spent on e-Learning products and services.[1] Compliance needs affect many employees and divisions within many organizations, and the use of e-Learning as an effective and widespread method for delivery is increasing.

Training is an integral part of an effective compliance program, and often one of the best strategies for issue prevention. When it comes to conducting business, what might be unethical or unlawful in the United States may be an accepted practice in other countries—or vice versa. As a result, employees of US-based businesses sometimes feel they must choose between losing business by rejecting local customs and winning business by violating US law. Having key people or all staff trained is vital.

Training with multiple touch points

Developing a program that provides a wide variety of learning tools on a regular basis includes online education, education alerts (one page tip sheets), e-mail educational reminders, newsletters, face-to face-training, etc. Organizations are using a blended approach, implementing online to cover the basics that everyone needs to know about, and then analyzing the online reporting to tailor their instructor-led programs. In this way, they can target the more complex or weaker areas, for example, where people might be struggling with certain concepts.

Tips for getting started – ask yourself:

- What are the learning objectives of the training?
- What is the compliance risk?
- How will the risk affect the employee or other stakeholders?
- How will this change the employee's routine (i.e., what's changed)?
- What are the consequences of inaction?
- Who is the target audience (e.g., new employees vs. seasoned employees, vendors, contractors, and third parties)? Are all employees affected, or a specific few?
- What roll does the audience have? Tailoring the learning experience to your audience will require different information, perhaps presented in a different way, to customize content for each audience.
- Start with clearly written guidelines, policy, and code of conduct.
  - Key issues: agents/consultants, commissions, gifts and entertainment, charitable contributions
- Customize course elements for the location
  - Local, relevant content
  - Policy and law differences
  - Images and branding
  - Workflow systems and process

Tips for designing and deploying the course

Once you have defined what your learners need to take away from your compliance course and how you will measure its success, you must decide how to put your course together. Consider these tips for successful compliance training design and deployment:

Continued on page 8

1. Find channels that will best achieve your intentions. The message and audience are key factors in deciding how to best distribute your compliance training. For example, if your remote sales staff needs to be trained in the field, consider a series of shorter mobile courses they can take on the go. Perhaps your Human Resources department needs an interactive demonstration on using new compliant software, so an interactive course would be best to capture software demonstrations and test hands-on knowledge. Assessing your audience and their individual learning needs will make a positive impact on compliance information retention.

2. Reach the widest audience possible. Development is only half the battle. If no one is able to take your training or if it is not motivating, your message efforts are wasted. After deciding where your learners will likely be taking the training, make it as accessible as possible. Give learners time to complete the training so it doesn't come down to last-minute mandates. Also give incentives for completing the training by letting them know how it is pertinent to their individual roles within your organization.

3. Make it easy to complete. Compliance doesn't have to be boring. A dry seminar, just reading new policies from a notebook, is unnecessary. Creating fun, interactive, and relevant training courses is key to generating interest and setting a precedent for employees to take future courses.

4. Empower your learner to become a stakeholder. Explain why and how this information is relevant to the learner to increase the odds that the learner will complete the course, retain the information, and incorporate it full circle into their daily work lives. Training must be seen as more than a mandatory corporate policy to be effective. Letting your audience in on their vested interests will increase your success.

5. Time is money, and brevity is key. Make sure your training only covers the most pertinent information, and that you are saying it in the most effective and concise way possible. Time spent developing long courses and time for each employee to participate in a lengthy course translate into time and money spent from the budget.

6. Make sure your content is relevant to each user. If different departments only need portions of information in your training, consider creating various shorter modules with a series of selection questions to direct the learner to the appropriate module for their training material.

7. Mix it up. Combine a blended approach to reinforce key learning concepts. The more occasions the learner has to engage and apply what they learn, the better they will retain the training. Consider a blended training approach that incorporates instructor-led lessons, web and mobile applications, follow up surveys, and social interaction with online blogs and chat.

8. Give real world examples. The way to really drive the urgency of compliance home is through relevant examples and real-world scenarios that the learner may encounter in the workplace. Give an example of the risk, explain a scenario where this may come up, and identify how to correctly address the risk.

9. Reinforce learning objectives through practice scenarios. If you need your employees to change their behavior or handle new risk situations differently, consider a highly interactive course that offers simulation or gaming. Training is a great, safe place to practice hypothetical scenarios and decision-making.

10. End with a bang. After your learner has completed the course is a key time to reinforce the importance of your message in real and tangible ways. Ending the course with a quiz may bring a sigh of relief that it's complete, but it is wasting a valuable opportunity to leave a call to action. Make sure you leave the learner with a strong final impression on why the training is important and provide concrete ways they can immediately begin implementing what they have learned.

Conclusion

Incorporating these design elements will provide quality training that fits your risk and compliance training needs. Once you've determined your training needs, outlined your content, and brainstormed ways to keep it fresh and interesting, you have to decide how you will develop and deploy your training. ✳

Editor's note: Chanin Ballance is co-founder and CEO of viaLanguage, one of the largest women-owned multilingual solutions companies in the country. She is constantly breaking ground on new technological landscapes, from mobile training solutions, machine and hybrid translation, to customized multilingual product launches in 32 countries. Chanin may be contacted in Portland, Oregon by e-mail at cballance@vialanguage.com or by telephone at 503-243-2007.)

Notes:

1 Patel, Laleh: "ASTD State of the Industry Report 2010: Continued Dedication to Workplace Learning," *Training & Development*, November 10, 2010. Available at http://www.astd.org/TD/Archives/2010/Nov/Free/1110_2010+State+of+the+Industry.htm

Fast Facts

Today, more fraud investigations are happening worldwide:

- More than $1 billion in fines were assessed for FPCA violations in 2010 (Report 2011)
  - BAE Systems (2010) - $400 million
  - Technip (2010) - $238 million
- Johnson and Johnson fined $70 million for overseas bribes by international orthopedic subsidiaries (R. C. Report 2011)
- Recent study shows that more than 70 public companies are currently under investigation
- US Department of Justice and US Securities and Exchange Commission now working together to enforce the FCPA.
- Other countries have anti-corruption initiatives:
  - UK Bribery Act – you can be liable for both (in US and UK)
  - US companies can be liable for penalties in Germany

Compliance is all about PEOPLE

CONTINUED FROM PAGE 5

have in place an appropriate, robust, effective compliance program that your employees—the people—can follow to keep your organization compliant. ✳

Editor's Note: Daniel A. Cotter is Chair of the Corporate, Transactional and Regulatory/Compliance group at Lindemann LLC in Chicago. Dan works with clients, both in-house and as an external attorney, in the development, review, and training on compliance programs and various elements within broader compliance programs. He is a frequent lecturer and writer on various substantive matters, including effective compliance. He can be contacted by e-mail at DCotter1@msn.com.

SCCE has stepped up our environmental responsibility by printing Compliance & Ethics Professional on recycled paper. The interior pages are now printed on paper manufactured with 100% post-consumer waste. The cover stock is made up of 10% post-consumer waste and is locally produced in Minnesota near our printing facility. In addition, the energy used to produce the paper is 100% renewable energy. The ink used in our magazine is 100% soy-based water-soluble inks. Certifications for the paper include The Forest Stewardship Council (FSC), Sustainable Forestry Initiative (SFI), and Green-e.org.

Managing conflicts of interest: The basics

By Meghan K. Daniels, CCEP

MEGHAN K. DANIELS

Conflicts of interest in the workplace occur when an individual's personal or private interests interfere or appear to interfere with his/her professional judgment or commitment to his/her employer. Conflicts of interest present a challenge for most organizations, because they can occur at any time, at any place, and at any level. Moreover, to complicate matters, the impact of a conflict of interest can range significantly, depending on the circumstances, which are rarely predictable. Often, what might seem like a minor issue can actually create significant harm to a company under the "right" mix of circumstances.

Given the breadth of and potential for conflicts of interest, it's best to have a thorough, yet practical, strategy for identifying and managing those conflicts. For example, at the same time conflict-of-interest policy and procedures are communicated to employees, Compliance offices need to be ready to address employees who present a higher risk. A more robust strategy, including targeted training and an annual disclosure process, may be needed. This article provides a practical guide to managing conflicts of interest, specifically for companies that have not yet developed a strategic approach to conflicts, or for those looking to revamp and reassess the process.

Step 1: Develop an effective conflict-of-interest policy

Employees can only follow the rules if they understand what the rules mean. As such, it is absolutely critical to develop and maintain a conflict-of-interest policy that is easy to read and easy to understand. Equally important, and recognizing that the subject has an inherent sense of ambiguity, the policy should not leave room for grey areas or an excessive amount of interpretation. Instead, the policy must clearly define the scope of the subject matter and, even more clearly, set out resources (including the compliance officer) that are available to employees when questions or concerns arise. Below are some practical suggestions for developing and maintaining a conflict-of-interest policy.

1. Focus your policy on your company's audience. Types of conflicts vary drastically, depending on a company's make up. Industry and employee population, among other factors, will often dictate specifics around conflicts management. For example, many intricate rules surround conflicts of interest in industries such as finance, academia, and healthcare, and in areas such as the public sector and government contracting. Those rules must be addressed accordingly, often in very detailed policies. In other industries, the objective is typically to provide examples that cover a broad spectrum of relationships and activities that can lead to conflicts of interest or the perception thereof. Although most conflicts of interest are financial in nature, it's imperative to emphasize that conflicts can come in many shapes and forms. Consider addressing the following areas in your policy:

- Investment and ownership interests
- Family relationships
- External activities and positions, such as Board service and secondary employment
- Gifts and entertainment

2. Identify your policy's applicability. Make sure that your policy clearly articulates to whom it applies. It's often as simple as an introductory sentence, such as "This policy applies to all employees, officers, and directors of the company."

3. Clearly define your terms. Given the subject matter, conflicts or the potential for conflicts are often described using terms that seem to be self-explanatory. Herein lies a recipe for ambiguity. By including a specific section that defines terms such as "financial relationship," "family relationship," and "ownership interest," you'll be saved from answering hundreds of questions down the line.

4. Include concrete examples. The easiest way to ensure that a policy is readable and easy to digest is through the use of applicable examples. Concrete examples are especially imperative when the specific policy applies to a general audience in other words, an audience that might not be used to thinking about or evaluating situations for potential conflicts.

5. Communicate your procedure for evaluating disclosures and your process for follow-up. Communication is essential for all stakeholders, especially members of the board of directors, officers, and members of senior management, in order to understand that the company will take conflicts of interest and the perception of conflicts very seriously. Equally important is communicating the need for transparency and disclosure. Your audiences must understand that, in the event of a conflict of interest, the organization has the responsibility to respond accordingly. That said, a policy should also clearly articulate that disclosing a relationship or an ownership interest does not always lead to an inherent conflict, but rather allows the company to take appropriate precautions to protect itself. The policy should, therefore, be clear on processes and procedures surrounding the disclosure of conflicts of interest or potential conflicts of interest so that employees know what to expect. The policy should also help employees understand that there are appropriate resources within the company (i.e., the compliance officer) who are responsible for evaluating disclosures accordingly.

PRACTICAL TIP: Consider drafting two policies

In some cases, it might be appropriate to create two conflicts of interest policies: one policy for the entire organization, including lower risk employees, and a more specific policy aimed at the Board of Directors and Senior Management. The general policy should outline day-to-day responsibilities with respect to conflicts of interest and may include relevant examples for the general population. A more specific policy should set forth procedures for formal disclosure and evaluation, as well as tailor examples specific to this higher-risk group. This approach often works when there is a strong likelihood of disclosures from members of the board of directors and senior management.

Step 2: Train and communicate the policy

A great policy can be lost if it's not effectively communicated and easily accessible by your intended audience—employees, members of senior management, officers, and directors. For this reason, it's essential that you take adequate steps to make your policy available to everyone and that you remind them of its importance on a routine basis. Some fundamentals include:

1. Make sure your policy is accessible by your intended audience.
   - Post your policy on your company's intranet site
   - Distribute your policy electronically to employees on an annual basis
   - Have hard copies available in the event they are requested
2. Remind employees about the policy on a regular basis.
   - Draft occasional newsletter articles reminding employees of the policy
   - Communicate with employees about conflicts of interest at certain times throughout the

CONTINUED ON PAGE 12

 CONTINUED FROM PAGE 11

year (i.e., the holiday season is ripe for gift-related issues)
   - Have hard copies available in the event they are requested.
3. Train employees on the concepts included in your policy.
   - Roll-out a course covering conflicts of interest
   - Include conflicts of interest as a topic in your annual Code of Conduct training
   - Discuss conflicts of interest at annual board of directors meetings
   - Conduct live training sessions to targeted audiences about the conflicts of interest policy
   - Have hard copies available in the event they are requested

Step 3: Deploy an annual disclosure questionnaire

Requiring members of senior management, officers, and members of the board of directors to complete an annual conflicts-of-interest disclosure questionnaire is essential to transparency and effective conflicts management. Fundamentally, a company is far better off discovering a conflict of interest and taking appropriate mitigation steps even if a conflict must be reported and investigated than the alternative. Below are some practical factors to consider when designing and/or reviewing your questionnaire:

1. Confirm that the questionnaire covers the scope of your policy. You have drafted your policy to include the aspects surrounding conflicts that are most important to your company. To that end, your questionnaire should comprehensively capture those elements. You never want to return to your audience to ask new questions simply because you neglected to ask a few things the first time around.

2. Make sure that the questionnaire is easy to use. One must assume that all individuals completing the conflicts of interest questionnaire would prefer to be doing just about anything else. With that said, make the experience as easy as possible for them. If the questionnaire is administered electronically, be sure that the tool is easy to use and is introduced with clear instructions. If the questionnaire is administered in hard copy, take the most basic steps and be sure that respondents have enough space to provide the background for affirmative responses when necessary. Also be sure that the questionnaire is always accompanied by the policy (either in hard copy or electronically).

3. Design your questionnaire so that it is comprehensive, but not overly burdensome. It is essential to ask not only the questions that satisfy all reporting obligations, but also the questions that provide the information needed for adequate assessment. Examples include: conclusions about independence of board members and officers, hiring and promotion decisions concerning members of senior management, and evaluations of policy and procedure violations. Because the questions could be endless, it's important that you ask what's required to elicit only the answers you need and take care not to ask three questions when one would suffice.

4. Deploy the questionnaire to an appropriate audience. In an ideal world, everyone at an organization would participate in an annual conflicts of interest disclosure. In reality, this approach is resource-intensive and not often necessary. Those employees with decision-making authority on behalf of the company primarily members of the board of directors, officers, and members of senior management are the most important audience to target. From there, it might also be advisable to target other groups based on either previously identified risks or previously disclosed conflicts of interest.

5. Emphasize the importance of the disclosure to your intended audience and your reasons for doing it. As the questionnaire process is often arduous and time consuming, make sure you highlight both the value of the annual disclosure and explain its purpose, and make sure your tone is both positive and appreciative.

6. Request review by outside counsel on an occasional basis. Given the ever-changing regulatory landscape, it's advisable to elicit outside counsel review of your policy on an occasional basis, especially when you become aware of any external changes that could impact your reporting obligations. External consultation is especially relevant if you are a not-for-profit organization privy to specific IRS disclosures or a company subject to other potential regulatory reporting requirements.

PRACTICAL TIP: Have your questionnaire mirror your policy

It often makes sense to divide your questionnaire in accordance with the set-up of your policy. For example, if the policy covers four areas (ownership and investment interests, family relationships, external activities and positions, and gifts and gratuities), the questionnaire should mirror those segments and should ask at least one, but often several, questions covering the defined areas.

Step 4: Summarize, analyze, and report on your findings

The information gained through an annual conflict-of-interest disclosure process loses most of its value if it's not properly tracked, summarized, and analyzed, with subsequent reporting and follow-up. Given the potential for a significant amount of data and the likelihood for situations that require complex analysis, it's imperative that you have a resource (e.g., as a technology tool, an external partner, or a dedicated in-house employee) to help tackle the administrative challenges associated with this type of event. Below are some practical guidelines to manage the disclosure process:

1. Track participant rates to ensure complete participation. Full participation by the targeted audience is essential for an effective disclosure process. Whether using an external partner or an internal resource to manage the deployment, be sure to have a procedure in place for verifying completion of the questionnaire and for subsequent follow-up with delinquent participants.

2. Create an effective system for summarizing questionnaire responses. Be sure that you have an efficient system for reviewing and summarizing questionnaire responses so that affirmative responses are clearly identified for purposes of subsequent analysis and follow-up. Whether it's a detailed report provided from an external partner, a technology solution, or a simple spreadsheet, this piece is essential.

3. Evaluate affirmative responses following review and summary of questionnaire responses. Once affirmative responses are identified, evaluate them on an individual basis. Depending on the person disclosing, your analysis could result in decisions which impact, among other things:

- committee placement for the board of directors;
- continued service on the board of directors of a public company; or
- the reporting relationships between members of senior management.

The results of your analysis will also often help you determine whether you have external reporting obligations, such as to the IRS or the Attorney General's Office.

4. Report disclosure results and analysis. Following your review and analysis, it is imperative to report the results of your findings to a governing body of the company, such as the full board of directors or, in some cases, the Audit Committee of the board of directors. Support from the board of directors on this initiative represents the company's commitment to transparency, but also provides heightened authority of the compliance officer to respond quickly and effectively to information attained through the process when, and if, necessary.

PRACTICAL TIP: Communicate the importance of disclosure

An easy strategy that emphasizes the significance of the annual conflicts of interest disclosure includes introducing the questionnaire with an opening letter from the Compliance Officer outlining the regulatory landscape and the requirement for

CONTINUED ON PAGE 15

 CONTINUED FROM PAGE 13

transparency, and thanking participants for their cooperation and dedication to the company.

Step 5: Extra credit

Even though the hard work is mostly complete, it is best practice to maximize the fruits of your labor through some additional follow-up steps, as suggested below:

1. Review disclosure summaries on a year-over-year basis. This step, although not mandatory, will allow you to trend and benchmark affirmative responses on an annual basis and will enable you to determine, for example, if there is a need for a policy revision or additional training in certain areas of the company. It's also a good idea to review feedback on specific questions (i.e., several respondents asked for additional guidance on question number 6), which will allow you to improve your questionnaire when possible. Reviewing the results of your analysis may also dictate whether you can remove questions in subsequent years or whether you should consider supplementing the questionnaire as you move forward.

2. Review and revise company policies based on disclosures. Your review of disclosures will often teach you about internal policies and procedures that might be ready for revising or fine tuning. For example, if several employees disclosed that they accepted gifts not consistent with your gift policy, this is a likely sign that the policy is not clear, not accessible, or poorly communicated. Use what you learn as an opportunity to improve your policies, procedures, and compliance program in general.

3. Conduct appropriate outreach to employees who made disclosures, even if further analysis revealed no conflict. Although this step might be obvious, follow-up is especially important in situations that have the potential for mitigation (e.g., a member of senior management can continue to serve on a certain board of directors provided that he/she recuses himself/herself when appropriate; or a gift can be accepted provided it's under a certain value threshold). The company's objective should always be to evaluate situations and seek solutions that protect the company while treating the employee fairly.

Conclusion

Creating an approach to conflicts of interest management that is both comprehensive and realistic will allow you not only to fulfill mandatory reporting requirements, but also to meet the challenge of ensuring that the company's ethical standards are communicated to employees, and that any potential violations or conflicts of interest are disclosed to and reviewed by the company's compliance officer. ✳

Editor's note: Meghan Daniels is Senior Director of Advisory Services at SAI Global in Boston. She advises clients on the implementation of best practice compliance and ethics programs. Previously, she managed the conflict of interest disclosure process and corporate compliance program for Blue Cross Blue Shield of Massachusetts, Inc. Meghan may be contacted by e-mail at Meghan.daniels@saiglobal.com.

Meet Fernando M. Caleiro Palma

Anti-Corruption Program Manager – South America at Archer-Daniels-Midland Company in São Paulo, Brazil

An interview by Adam Turteltaub



AT: First, could you tell us a bit about your background before you got into Compliance?

FP: I graduated from law school in 1998, with a postgraduate in Civil Litigation in 2002. I have practiced law since graduating, and spent most of these years working in law offices in São Paulo.

AT: When did you join Wal-Mart, and what were your responsibilities there?

FP: I had the opportunity to join the team of Wal-Mart Brazil in February 2006 as Senior Attorney. At that time, my primary responsibility was the conduct, management, and preparation of contracts signed by the company in Brazil, as well as the structuring of the sector.

Like other corporate environments, where the Law department serves as support to other areas of business, my challenge in that period was also the integration with other areas responsible for supporting the retail business, serving as support for the Strategic and Corporate Affairs, Government Relations, Development, Marketing, Systems, and Real Estate departments. Later I was promoted to Legal Manager of Wal-Mart for the Southeast Region of Brazil, this time giving direct support to the Operations area of the company.

It was a fantastic and unforgettable experience, because I had the opportunity to not only work with highly competent professionals, but also learn the dynamics of business operations and the need for teamwork to support internal customers.

AT: You worked in the U.S. for Wal-Mart. What led you to come to the States?

FP: Wal-Mart had excellent opportunities for professional development, and I wanted to be ready should they appear. And they appeared.

Wal-Mart had a program that was called Global Talent Pool and one of the goals of this program was to provide opportunities for employees around the world to gain experience as an expatriate working directly at the company headquarters, located in Bentonville, Arkansas. In January 2007, I was chosen by the company to participate in this program. In April of that same year, my wife Fernanda Palma and I moved to the United States.

AT: What led you to a Compliance role?

FP: Wal-Mart Brazil already had a compliance structure integrated into the legal team and under the same line of reporting, so the interaction was constant. Gradually, I understood the real need to have a compliance program that is structured and robust, with clear policies and procedures, and that is sustainable and evolving, not only to suit the real needs of the company, but also to adequately address the challenges of the sector.

AT: What were some of the key compliance challenges you saw?

FP: Unfortunately we still see companies who treat compliance as "a necessary evil." In conversations with colleagues in other organizations, I see that integration and partnership with the business areas remain a challenge.

What seems like an excellent business opportunity for the company may, at the same time, present a risk from the perspective of compliance. It is precisely this scenario that underscores the value of employee training, because many times we find that missteps are simply the result of ignorance of existing policy. So, I think it's important to support the dissemination of the rules and to always be ready to support the business as it evolves and grows.

AT: You left Wal-Mart, went to a law firm for a while, and then went to Archer-Daniels-Midland Company (ADM). What attracted you to working at ADM?

FP: I left Wal-Mart in April 2010 to join the law firm Machado, Meyer, Sendacz & Opice Advogados. My primary role there was to lead real estate due diligence in merger and acquisition transactions sponsored by the law office.

In September of 2010, ADM invited me to join the company's Office of Compliance and Ethics and lead their anti-corruption programs in South America.

Once again, my career would take a new direction, and I was very happy about it, because the role seemed an excellent opportunity to support ADM's efforts to maintain its high business standards in South American countries.

AT: How does ADM organize its Compliance department?

FP: ADM has a solid structure in the Compliance area, with more than 110 professionals in the Office of Compliance and Ethics (OCE), which is based at the company's headquarters in Decatur, Illinois. OCE is comprised of the following areas: Commercial Compliance, Product Quality, Regulatory & Scientific Affairs, Employment, Risk Management, Programs, Environmental, and Health & Safety. In the pillar of Commercial Compliance, to which I belong, we have the following responsibilities: Develop new policies and procedures; develop and deliver training courses; investigate complaints; act as a resource to stakeholders; interface with regulators; and implement controls and monitoring. I am focused on the implementation of the company's global anti-corruption program in South America.

AT: What led the company to create a Compliance role dedicated just to anti-corruption compliance?

FP: ADM is a global company that works to achieve the right results the right way. The complexity of international business operations and the differences in cultures around the world led the company to develop a global network of local compliance officers who assist local managers and help ensure that the highest levels of business integrity are maintained throughout all of ADM's operations.

AT: What are your responsibilities in that role?

FP: My primary role is managing the company's anti-corruption program in South America. I also provide assistance to other initiatives in this region, including antitrust, U.S. trade restrictions and embargoes, Customs compliance, and privacy laws.

Our initial objective in South America was to identify all the companies that directly or indirectly acted with government agencies on behalf of ADM, (for example, Customs agents) and put them through a certification process to ensure that these companies operate with the levels of integrity expected by ADM. In Brazil, we have four professionals dedicated exclusively to screening the partner companies of ADM.

CONTINUED ON PAGE 19

 CONTINUED FROM PAGE 17

As I usually say, compliance is a marathon, not a sprint. The challenges are constant, and we have to be ahead of the curve in order to identify them, mitigate them, treat them, and finally educate the business areas of the risks in this sector, so that we are sure that ADM's business is always conducted in accordance with the highest levels of integrity.

AT: How do you coordinate your activities with those of the rest of the Compliance team?

FP: On a regular basis, we report to our OCE colleagues on the screening process. We share information through a global database. We have instant visibility into the screening process for each of the roughly 300 companies that are currently going through the process in South America. This is fundamental to the success of the operation.

AT: What are some of the anti-corruption risks faced by a company dealing in commodities?

FP: ADM connects the harvest to the home and transforms crops into products that serve vital needs for food and energy. At more than 240 processing plants, ADM converts corn, oilseeds, wheat, and cocoa into products for food, animal feed, chemical, and energy uses. ADM also operates the world's premier crop origination and transportation network, connecting crops and markets in more than 60 countries. So, it is indeed a complex and challenging business. The sourcing and transportation of crops can often require Customs clearance, and I work to ensure that this process is conducted in accordance with the applicable laws and procedures.

AT: ADM also has processing plants in Brazil that produce goods ranging from cocoa powder to biofuels. Are the compliance challenges different there than in the raw commodities business?

FP: In an environment as diverse as ADM's, compliance solutions must be developed to suit every need. When we buy soybeans and cocoa, we interact directly with the grower, so we face specific challenges and obligations. When it comes to biodiesel, we regularly and directly interact with government agencies, presenting a different set of challenges and obligations. There is no one-size-fits-all solution. And understanding the business of the company is vital to developing effective compliance solutions.

AT: What has ADM found to be effective for mitigating those risks?

FP: The partnership with the business areas is essential for risks to be quickly identified, addressed, and mitigated. Without this integration, it is difficult for a program to be effective. It's also important to weave controls across functions, such as Finance, Procurement, and Internal Audit.

AT: There has been a lot of activity to stem corruption in Brazil and across the region. Are you seeing much progress?

FP: Absolutely. In fact, as a Brazilian citizen, I am very pleased to see initiatives by both government and business.

AT: I was struck by the amount of interaction among the attendees at the SCCE São Paulo Compliance Academy. It seemed as if everyone already knew each other. Do compliance professionals talk with each other a great deal in Brazil? Is this translating into collective action to stem corruption?

FP: Increasingly, we see new events, conferences, summits, and roundtables to discuss the industry and its challenges. There is good integration among the professionals, and everyone benefits from that. Benchmarking and shared best practices are important tools to learn new solutions, and this can only happen through interaction with other colleagues. ✳

Editor's note: This interview was conducted by Adam Turtletaub, Vice President of Membership Development for SCCE. Fernando Palma can be contacted by e-mail at fernando.palma@adm.com and Adam can be contacted at adam.turteltaub@corporatecompliance.org.

Speaking for our profession

By Roy Snell

It's stunning how many people feel qualified to speak for compliance professionals. People who have spent their career in ethics, audit, risk, legal, etc., all seem to think they should define our profession. When is the last time someone with no legal experience spoke for the legal profession? Why are these people telling the world how a compliance program should be defined? I'll admit, some of it's good for us. Any press is good press. The fact that everyone wants in on the act is a positive indication that what we are doing is at least interesting. Despite all that, damage is being done. People who have never been compliance professionals are likely to give bad information to others about what the job involves. And some of them are intentionally trying to manipulate the definition of our profession and compliance programs to their advantage.

There are people giving presentations about our job who have never held our job. We have people communicating with the enforcement community who have never spent a day managing a compliance program. We have people with very little experience writing several hundred page descriptions of compliance programs and whose motivation is to make money. We have people coordinating "compliance conferences" who could not identify a qualified compliance professional if their lives depended on it. And then there are the articles. We have 35-year veterans of other professions writing articles suggesting that compliance officers should report to the general counsel. This is against almost every piece of advice the enforcement community has served up. Some of these people have resumes (from their profession) that would cause many people to actually believe what they say. This is irresponsible. This is the equivalent of a risk manager giving legal advice, or an ethicist telling an auditor how to do business. It just doesn't happen. We should not allow this to happen to us.

And then there is academia. Theoretical solutions to this serious problem are not helping. These people are telling their students—our future leaders—that all you have to do is talk about doing the right thing and all your problems will be solved. There is no emphasis on finding, fixing, and disciplining. An overwhelming number of business schools teach no compliance course whatsoever. Sure, talking helps many people, but it doesn't help all the people and to imply that talking is all you need to do is a crime.

Some mean well. Some don't know what they don't know. The compliance profession is new and exciting; everyone wants to get in on the act. I understand. Compliance looks simple. I guess that has given them some confidence. Maybe they assume we need help. That can happen when you have no experience and a lot of confidence. There is a disconnect.

They feel strongly about it. Risk guys want compliance to be all about risk; ethics guys want it to be all about ethics; lawyers think it's all about the law, etc. If that were true, society's loss of confidence in business and business leaders would have been solved long ago. They want to push their specialty. If it was all about, "fill in the blank," we would not need compliance programs and compliance professionals. These other subspecialties have been around for 50 years. Pushing the methodologies of the past is dangerous. They didn't prevent wrongdoing then and they can't now. And society is fed up with business.

What compliance programs are all about is the use of many tools in concert to prevent and find problems and fix the problems we find. These people want control of compliance programs, or at least control the definition of compliance programs. And yet, when there is a problem to fix that may involve big disappointment and possibly discipline, these people can be found hiding under the table, where they have been for 50 years.

Some would rather we didn't look for problems at all; instead they want to wait, see if we get caught, and then defend it. That is a paradox. Our profession was created because those who came before us failed to look for, find, and fix problems. Now they want to tell us how to do it. This is dripping with irony. All the while, the press, the public, and the politicians are fed up with corporate America because we can't seem to find and fix our own legal and ethical problems. It would be funny if it weren't such a travesty.

Compliance works because we use a balanced approach to all of the compliance tools. It's a very difficult job and business leaders need to be told how compliance works by people who actually have done the job. What people don't understand is how difficult the job is. The guys who have been hiding under the table when problems occurred in the past don't know how difficult it is to solve the problems you find. If they would have looked for, found, and actually fixed all the problems, they would know how tough this job is. They don't know how important having access to leadership and the support of leadership is. They don't know how important collaboration, negotiation, motivation, and other "people skills" are. They don't know how difficult it is to manage a whistleblower complaint about leadership. They don't know what it's like to wake up at two in the morning thinking "What if the government finds a problem that I should have found?" They don't know what it's like to make someone who is already busy add another step to their process. They don't know what it's like to have to force everyone to attend education. They didn't get it done and they don't know what it's like; and yet they insist on telling everyone how compliance programs and our profession should be defined. The arrogance of it all. It's maddening.

The only reason they keep doing it is because no one stands up to them. We don't stand up because we are a young profession. We don't talk about this because people are too nice. Most of all, you are all more humble about our profession than I am. My real problem is that I am impatient. I want everything done yesterday.

Here is my advice to compliance professionals: Stand up and do something about this. When you see some group trying to define your profession, who has never been in your profession, call someone involved and let them know what you think. Write about it. Speak about it. Mention it in your social media circles. The more we let the emperor know that he has no clothes, the more he is likely to stop. ✳

If you have any questions that you would like Roy to answer in future columns, please e-mail them to: roy.snell@corporatecompliance.org.

Compliance & Ethics Professional

CONTACT US!

www.corporatecompliance.org

service@corporatecompliance.org

+1 952 933 4977 or
888 277 4977 (ph)

+1 952 988 0146 (f)

Society of Corporate Compliance and Ethics
6500 Barrie Road, Suite 250
Minneapolis, MN 55435

To learn how to place an advertisment in Compliance & Ethics Professional, contact Wilma Eisenman:

wilma.eisenman@corporatecompliance.org

+1 952 933 4977 or 888 277 4977

Complying with The California Transparency in Supply Chains Act 2010

By Susanne Gebauer

SUSANNE GEBAUER

On September 30, 2010, former Governor Arnold Schwarzenegger signed The California Transparency in Supply Chains Act 2010 (Senate Bill 657) into law. Section 1714.43 in the California Civil Code goes into effect on January 1, 2012. The Act requires retail sellers and manufacturers that do business in California and have worldwide gross receipts exceeding $100 million (US) to publicly disclose their efforts to eradicate slavery and human trafficking from their direct supply chains for tangible goods offered for sale. According to an estimate by the California Franchise Tax Board, around 3,200 companies will be affected by this Act. Indirectly, the Act will also affect thousands of suppliers and vendors along the supply chains of these large retailers and manufacturers.

Background on the Act

Senate Bill 657 was put forward by Senate President pro Tem Darrell Steinberg (D-Sacramento) with the Alliance to Stop Slavery and End Trafficking (ASSET) as the source and the Coalition to Abolish Slavery and Trafficking (CAST) as the co-sponsor. The not-for-profit organizations that sponsored and rallied for the Act argued that it would create an opportunity for California companies to demonstrate leadership in eradicating slavery and human trafficking from their supply chains and empower consumers to reward companies that proactively engage in such efforts.

As opponents of the bill, industry associations such as the California Grocers Association (CGA) and the California Manufacturers and Technology Association (CMTA), argued that the lack of resources—especially on the side of grocers—would prevent them from monitoring supplier employment. Furthermore, the associations noted that the bill provides no details as to what constitutes compliance with the legal requirement. This last point of criticism will become apparent when reviewing the legal requirements.

Who needs to abide by the Act

Every retail seller and manufacturer who does business in the state of California and has annual worldwide gross receipts that exceed $100 million for taxable years beginning on or after January 1, 2011 needs to abide by The California Transparency in Supply Chains Act. (The 2011 tax returns will be used to identify who needs to comply when the Act goes into effect in 2012.) Definitions of "retail seller," "manufacturer," "doing business in California," and "gross receipts" are referenced and provided for in the California Revenue and Taxation Code. These definitions concern the type of activity, investments, and financial gain in the state of California. Legal counsel should be consulted to evaluate the applicability of this Act.

How to disclose

If the company has an Internet website, the public disclosure should be posted with a "conspicuous and easily understood link" on the homepage. In cases where the company does not have a website, the written disclosure shall be provided within 30 days to consumers who make a written request for it.

The legal text does not provide any details on how to present the disclosure. It is unclear to what extent the Act actually needs to be mentioned or how a link can be made "conspicuous." That is, should the link be named "The California Transparency in Supply Chains Act," "Eradicating Slavery and Human Trafficking in our Supply Chain," or can it be a more general title such as "Corporate Social Responsibility?"

Furthermore, once one clicks on the link on the homepage, it is unclear whether to disclose the information on the ensuing page or whether it can be incorporated into a document, such as a corporate social responsibility report. These items and the topics required to be covered in the disclosure (detailed below) are some of the compliance problems that companies have confronted.

What to disclose

Companies need to disclose to "what extent, if any" they engage in the five following activities:

- **Verification**

  Engagement in verification of product supply chains to evaluate and address risks of human trafficking and slavery. The disclosure shall specify if the verification was not conducted by a third party.
- **Auditing**

  Evaluate supplier compliance with company standards by auditing for trafficking and slavery in supply chains. The disclosure shall specify if the verification was not an independent, unannounced audit.
- **Certification**

  Requirement of direct suppliers to certify that materials incorporated into the product comply with the laws regarding slavery and human trafficking of the country or countries in which they are doing business.
- **Internal accountability**

  Maintenance of internal accountability standards and procedures for employees or contractors failing to meet company standards regarding slavery and trafficking.
- **Training**

  Company employees and management who have direct responsibility for supply chain management must receive training on human trafficking and slavery, particularly with respect to mitigating risks within the supply chains of products.

None of the terms used in these requirements have been defined. Important definitions for terms such as "direct supplier," "slavery" and "human trafficking" are missing from the legal Act. The California Attorney General has been contemplating holding a multi-stakeholder roundtable later this year to discuss the difficulties companies have been facing with the Act and issuing guidelines for legal compliance with the Act thereafter. If guidelines are issued, they will most likely be presented after the Act comes into effect on January 1, 2012. Thus, currently, as the industry associations pointed out in their criticism of the Act, the details as to what constitutes compliance with the legal requirements are missing. Nevertheless, some recommendations for assessing the scope of a company's engagement in activities to eradicate slavery and human trafficking can be made.

Evaluating the extent of your activity

Although the legal text does not provide definitions for verification, auditing, certification, internal accountability, and training, common perceptions exist on what these activities consist of in the realm of supply chain management.

Verification: A general risk assessment of the supply chain can be conducted in order to identify the risks of slavery and human trafficking in a specific supply chain and the possible action to address said risks. The product sourced or manufactured, the location of the sourcing activity, and the type of labor involved are

CONTINUED ON PAGE 25

CONGRATULATIONS to CCEP designees!

CCEP®
Certified Compliance & Ethics Professional

The Compliance Certification Board offers you the opportunity to take the Certified Compliance and Ethics Professional (CCEP) certification exam.

Achieving certification has required a diligent effort by these individuals. CCEP certification denotes a professional with sufficient knowledge of relevant regulations and expertise in compliance processes to assist corporate industries in understanding and addressing legal obligations. CCEPs promote organizational integrity through the development and operation of effective compliance programs.

Questions? Please contact:
Liz Hergert at +1 952 933 4977, 888 277 4977
or ccep@corporatecompliance.org

Mojola K. Adewumi
Sarah E. Agnetti
Janet M. Akers
Cindy A. Anderson
Nicole M. Angell
Russell G. Ball
Cecelia M. Ball
Amanda Bill
David N. Bourne
Cathi Bowman
Ana M. Buitrago
Reina F. Cabatana
Molly A. Campos
Thomas Carague
Antonio A. Caram
Deann F. Carr
Salvatore J. Ceraolo
Ronald L. Change
Nadia M. Ciaravino
Alana A. Cook
Karly N. Coyle
Cheryl R. Cravens
Andrew D. Dixon
Matthew J. Doherty
Alan J. Douglass
Laura Ellsworth
Scott A. Ernst
Sarah C. Evans
Jan M. Festa
Jessica S. Foster
Joyce M. Foulke
Christiana Franchet
Kathleen E. Gibbs
Karen D. Green
Lauraine M. Guarino
Andrew C. Hall
Aimee C. Hawkins
Franklin J. Hesselroth
Kimberly Swain Higgins
Kathleen N. Hirose
Kathleen E. Holt
Matthew J. Hudock
Jeff S. Hunter
Christopher E. Jeffrey
Beth A. Katzenberg
Phoebe K. Kleiger
Anne F. Klezek
Thomas J. Kopera
John P. Kunkel
Corinne Lanuti
Colleen M. Larson
Robert M. Le
Carmel M. Liberman
Jack K. Matens
Troy J. McAlister
Dean L. McInnis
Katherine L. Meyer
Russel W. Mountjoy
Devin J. Needham
Eric S. Newman
Cathy L. Palmer
Tia M. Panch
Avani C. Patel
Caroline A. Preston
Jay G. Reilly
Nancy C. Riley
Greg Rotatori
Michele D. Rubincam
Cynthia L. Scavelli
Elizabeth S. Schwartz
Jerome R. Serwa
Lori Silver
Thomas M. Simms
Sarah R. Soifer
Rosanne Stanford
Kristen Stevens Sickle
Kerri A. Sweeney
Tamara B. Tait
Mark E. Thompson
Peter A. Timpano
Lisa A. Totten
Tanya D. Towns
Lisa A. Volo
Mechelle Warner
Greg Wilder
James A. Willobee
Christopher Wingert
Heather G. Woods
Tanya L. Wooten-Malone
Janis K. Young

 CONTINUED FROM PAGE 23

important factors to consider in such a risk assessment. Best practice is to engage a third party for the assessment.

Auditing: Regardless of the risk, audits can be conducted in order to examine compliance with laws in a company's supply chain. Most companies, however, will take the results of the risk assessment and identify high-risk areas to perform due diligence. Audit activity should be based on company standards set for suppliers. This means in order to address slavery and human trafficking in audits, company standards should include these aspects. Best practice is to engage an independent party to conduct the audits and enter the supplier's facility unannounced.

Certification: It is important to set up contractual obligations with suppliers to create a framework for compliance with company standards on slavery and human trafficking. Furthermore, suppliers should be performing due diligence with regard to their own suppliers and ensure that the suppliers further down the supply chain are complying with local laws on slavery and human trafficking. This due diligence activity by the supplier can be required by the company through supplier agreements or terms and conditions.

Internal accountability: Not only for external stakeholders, but also for internal stakeholders such as employees and contractors, a company should set standards on slavery and human trafficking and introduce internal procedures to verify compliance with the company's standards.

Training: Employees who have direct responsibility for supply chain management, such as buyers, engage with suppliers and make decisions on entering new business relationships on a regular basis. Through training, they should be made aware of the risks of slavery and human trafficking and on ways to mitigate those risks specific to the company's supply chain.

In complying with the Act and writing the disclosure, the aforementioned activities and the extent to which a company engages in such could be taken into account. These are only recommendations to consider for the disclosure, because legal definitions have not been provided yet.

Beyond legal compliance

The activities to be considered in the disclosure statement have been identified as best practice activities with regard to supply chain management. Keep in mind that the supporters of the Act are advocacy groups campaigning against slavery and human trafficking, and these activities are the demands they are placing on the private sector. Legally, a company is not required to engage in any of the above listed activities; however, with public disclosure comes the increasing awareness of the risks of slavery and human trafficking in supply chains, increased demand for positive action, and thus, pressure on companies to go beyond legal compliance.

Advocacy groups have already been engaging in benchmarking activities to evaluate supply chain management. These evaluations have been shared with the public in support of transparency and consumer empowerment. If a company is contemplating publicly disclosing its inactivity in the eradication of slavery and human trafficking from its supply chain, it should be prepared for "naming and shaming" by civil society actors. The supporters of the Act may well use the public disclosure to raise awareness for their cause.

Editor's note: Susanne Gebauer is Senior Researcher at STR Responsible Sourcing in Los Angeles. She manages corporate social responsibility projects related to benchmarking, code of conduct, and CSR program development. She also advises clients on legal compliance and supply chain risk. Susanne can be contacted by e-mail at susanne.gebauer@strrs.com.

Compliance and Social Media

By Frank Geovannelo, CCEP

FRANK GEOVANNELO

"If you are not using Social Influence Marketing in your job, please get started".[1] This sentence, taken from Razorfish's Employee Social Influencing Marketing Guidelines, makes the topic of using social media in the workplace appear to be a simple and noncontroversial one—but is it? The advent of Facebook, Twitter, and other social media sites has revolutionized the way we connect with each other. Earlier this year, Facebook celebrated its sixth birthday, and surpassed the 400-million user milestone. Of these users, 50% log in on any given day, almost 9% update posts each day, and each has an average of 130 friends.[2] Additionally, many users have profile information as well as personal pictures readily available to other Internet users.

This popularity has contributed to the tension between employees' and employers' perceptions regarding freedom of speech. The issue of freedom of speech is not new to the workplace. For example, in 1966 the Alaska legislature enacted Stat. § 14.20.095. The statute "recognizes the rights of a teacher to engage in comment and criticism outside school hours, regarding school personnel, members of the governing body of any school or school district, any other public official, or any school teacher, to the same extent that any private individual may exercise the right." However, due to the current opportunities for interaction through social media sites and the public nature of this interaction, the lines between what communications are protected and not protected have become less clear. This is especially true when employees are off-duty and share their personal thoughts about their workplace.

Employers are struggling with the rise of social media. On the one hand, some welcome the opportunity to interact with the general public and their customers. On the other hand, companies are struggling with the additional complexities social media sites bring to their job. Most compliance professionals recognize that social media sites can offer their companies the opportunity to assist with recruiting efforts, share best practices, and to network with like-minded peers. However, many may not recognize that there are times when using and monitoring social media sites may impede the rights of others.

Privacy

Interacting with others on social media sites can be addictive to some employees—both during work and off-duty. In general, if an employee expresses themselves and their opinions using social media, they cannot claim a reasonable expectation of privacy in their exposure.[3] Still, some employees feel they are entitled to some form of privacy when using social media sites and that their employer should not monitor their on-line activities. Deloitte LLP's 2009 Ethics & Workplace Survey found a big gap between employers and employees on whether businesses should be able to monitor Internet behavior off the clock. According to the survey, 60% of the business executives surveyed said they had a right to know how their organizations were portrayed by employees in online social networks, as opposed to 53% of employees who said that information was private.[4]

Some Facebook users may have a friend whose profile picture is of them wearing a Budweiser twelve-pack box on their head. While most of these instances of juvenile fun can be attributed to an innocent lapse in judgment, they can also be viewed by recruiters. A recent survey found that 63% of employers viewing social media site profiles have rejected candidates based on information found within those profiles.[5] Companies following such practices must be mindful though of not misusing information associated with protected classifications. User profiles tend to reveal more about the candidates than what recruiters are legally allowed to ask. Because of this, employers need to document exactly how they are using social media sites to find potential job candidates. Specifically, they should state what categories of information they monitor and how they use this information in their selection process. Lastly, companies that use social media sites as a method for identifying potential candidates should segregate the employees who search the sites from those who make hiring decisions.

Employee harassment

Social media sites allow us to communicate with a large number of people on an immediate basis. When a user of a site chooses to post a derogatory statement about another person, such action can constitute harassment. The complexity of such occurrences can initiate a workplace harassment claim for several reasons. First, a text message can easily be misinterpreted, because it does not allow for the subtleties of a face-to-face discussion. Second, social media sites allow users to post pictures of themselves and others, pictures they may not feel comfortable sharing with coworkers. Third, as most people "friend" their coworkers, many of these pictures can fall into the wrong hands and instigate comments—some of which may be unwelcomed. The unwelcomed comments can then lead to allegations of harassment. Most comments may not be severe or pervasive enough to create a "hostile work environment," but courts typically base their decisions on whether the company was aware of the comments and what actions were taken to address them.[6]

Online retaliation

Working conditions can lead to various levels of satisfaction. When satisfaction levels are low, employees often feel the need to vent their frustration about their employer. Because of this, there have been several instances of employees experiencing harassment or retaliation due to online activities. For example, in what is viewed as a ground-breaking case involving employees and social media, late last year the National Labor Relations Board (NLRB) accused American Medical Response of Connecticut of illegally firing an employee after she criticized her supervisor on her Facebook page. The company accused her of violating a policy that bars employees from depicting the company "in any way" on Facebook or other social media sites. The NLRB pursued this case, because the National Labor Relations Act (NLRA) prohibits employers from punishing workers, whether union or nonunion, for discussing working conditions or unionization. The NLRB said the company's Facebook policy was "overly broad" and improperly limited their employees' rights to discuss working conditions among themselves. Accordingly, the NLRB facilitated a settlement between the terminated employee and the company. Under its terms, the company agreed to revise its overly-broad rules to ensure that they do not improperly restrict employees from discussing their working conditions.[7]

Unintended consequences of employee communications

Employees and employers are beginning to recognize the immediate impact of social media sites. Prior to the birth of computers, the dissemination of public information was limited to media vehicles which either had inherent checks and balances for its content or predictable audience reach patterns. The dissemination of information from social media

Continued on page 28

 CONTINUED FROM PAGE 27

sites is analogous to a bomb explosion from which it is difficult to predict where all the debris will land. Recently, an employee of a social media agency, whose client was Chrysler, was fired for his tweet. The tweet read, "I find it ironic that Detroit is known as the #motorcity and yet no one here knows how to f****** drive."[8] The tweet was removed from @ChryslerAutos shortly thereafter, but the employee responsible for posting the tweet was fired. Chrysler did not demand the employee be fired, but it did say it will not renew its contract with the agency for the rest of this year.

This occurrence demonstrates that employers have a legitimate business interest in monitoring social media site traffic. By doing so, an employer can proactively protect their reputation and reduce legal risks. Some states, such as California, offer protection for individuals against privacy infringement from both public and private entities.[9] For employees in California, if their off-duty Internet conduct does not relate to their employment, then any discipline based on their Internet conduct would most likely be a violation of the employee's protected privacy rights. Colorado, North Dakota, and New York also have extended protection to those who engage in any lawful behavior unrelated to their employment.[10]

Collectively, these examples, and others, highlight the complexity of this topic. In some geographies, such as California, there are formal barriers for companies taking action on their employee's off-duty activities. For the remaining geographies, there exists a patchwork of legal opinions and laws that provide murky direction for employers. Regardless, there are some steps companies can take to help mitigate the risks associated with social media.

Social policy

As the use of social media sites has exploded in growth, so has the need for companies to respond and set guidelines. These guidelines should consider processes for the approval of company-sponsored messages on social media sites as well as guidance for employees who may be tempted to comment on company-related activities. For large companies, it may be difficult to achieve this spirit of compliance due to multiple cultures and social media user habits. Still, clear direction should be developed and communicated to employees.

So what elements should be included in a social media policy? Sharlyn Lauby, president of Internal Talent Management (ITM) which specializes in employee training and human resources consulting, suggests the following policy themes:[11]

- Introduce the purpose of social media. (What should the readers take away?)
- Be responsible for what you write. (Exercise good judgment.)
- Be authentic. (Be clear if you are representing your own thoughts or the company's.)
- Consider your audience. (Remember that current/past/future clients and other key stakeholders read your messages.)
- Exercise good judgment. (Read your tweet twice before hitting "send" and ask yourself how it may be received.)
- Understand the concept of community. (Add value to the online conversation about issues, topics, and concerns.)
- Respect copyrights and fair use. (Make sure you have the right to use something before you publish it.)
- Remember to protect confidential and proprietary info. (Loose lips sink ships…and possibly your job.)
- Bring value. (Be perceived as a contributor of new ideas and fresh thinking or one who can quickly solve problems as they are reported.)
- Productivity matters. (Remind employees not to waste time mindlessly trolling social media sites.)

In addition, companies can consider several other factors when implementing a social media policy. First, it is important that the policy does not appear to be too legalistic. Ideally the policy should clearly establish to all employees the boundaries of what an employee can and can't do. This includes providing direction for who can provide comments on behalf of the company as well as the process to approve company sponsored online messages and branding.

Second, the policy should be effectively shared with all employees. Simply placing a policy on the desk of all employees is not enough. A well-designed communication plan, backed up by a training program, helps to make the policy come to life so that employees understand not just what the policy says, but how it impacts them.

Third, managers need to proactively spot inappropriate activity and coach their employees on what online behavior is not acceptable. Fourth, the Information Technology (IT) and Compliance departments have a vital role to play in the administration of social media policies. The IT department should develop clear protocols for how they monitor social media sites and the Compliance department should provide clear direction for managers for how to respond to allegations of non-compliance activities.

Lastly, polices should not improperly restrict employees from discussing their wages, hours, and working conditions with co-workers and others while not at work.

Summary

Employees' use of social media sites, both on and off duty, will continue to challenge companies. Employers need to have a voice in this dynamic medium and also need to be confident that their employees know their boundaries when interfacing with social media sites. At the same time, compliance professionals need to recognize that until there are several more landmark legal decisions in this area, they need to proceed cautiously when considering disciplinary actions based on what they find on such sites. Employers and employees can find harmony on this topic, if they collaborate to address circumstances when personal freedoms and corporate risks intersect. By identifying these touch points, employers can develop policies and training that minimize the grey areas associated with this topic. ✳

Notes:

1 Razorfish: Razorfish Employee Social Influence Marketing Guidelines. 2009. Available at http://www.razorfish.com/img/content/RazorfishSIMguideWebJuly2009.pdf.

2 Crum, C: "How Over 400 Million People Use Facebook." 2010. Available at http://www.webpronews.com/how-over-400-million-people-use-facebook-2010-02.

3 Abril, PS: "A (My) Space of one's own: On privacy and online social networks." Northwestern School of Law *Journal of Technology and Intellectual Property*, 2007;6(1), 73-88.

4 Jourdan, J: "Employer Internet monitoring meeting resistance." *The Washington Post*. (June 27, 2009). Available at http://newman.richmond.edu:2435/hottopics/lnacademic/.

5 Davis, DC: "My Space isn't your space: Expanding the Fair Credit Act to ensure accountability and fairness in employer searches of online social networking services." *The Kansas Journal of Law and Public Policy*. 2006;16, 237-256.

6 Post or Perish: "Court Dismisses Employee Allegations of Facebook Harassment." September 16, 2010. Available at http://postorperish.com/2010/09/16/facebook-harassment-hostile-work-environment-jabbar-v-travel-services-inc/.

7 National Labor Relations Board: "Settlement reached in case involving discharge for Facebook comments." February 2011. Available at http://www.nlrb.gov/search/nlrbsearch/facebook.

8 Michalik, A: "Employee, agency fired over Chrysler f-bomb tweet." March 11, 2011. Available at https://www.examiner.com/auto-industry-in-san-jose/employee-agency-fired-over-chrysler-f-bomb-tweet.

9 Betzel, M: "2005-2006 privacy year in review special topic: Privacy law developments in California" [Electronic version]. Ohio State University I/S: A Journal of Law and Policy for the Information Society. 2006;2, 831-875.

10 Bosch, J: "None of your business (interest): The argument for protecting all employee behavior with no business impact" [Electronic version]. *Southern California Law Review*. 2003;76, 639-662.

11 Lauby, S: "10 Must-Haves for Your Social Media Policy." June 2, 2009. Available at http://mashable.com/2009/06/02/social-media-policy-musts/.

Editor's note: Frank Geovannello is Compliance & Integrity Manager, at Altria Client Services in Richmond, Virginia. He provides compliance services including the development of compliance risk assessments, development of compliance plans, creation and revisions of policies, and training development. Frank may be contacted by e-mail at Frank.M.Geovannello@altria.com.

Social media use, policies, and compliance professionals

By Roy Snell

RS: Eric, please explain your role as a social media manager for the compliance profession.

EN: As Social Media Manager for HCCA and SCCE, I manage HCCAnet/SCCEnet, a social network specifically for compliance professionals. I also manage the content in our LinkedIn groups, Facebook pages, and Twitter accounts, which are all great places to get answers and meet compliance pros. In addition, I have the opportunity to speak at various compliance conferences on how compliance professionals can use social media to advance their profession.

RS: Please tell us what benefits Twitter provides and what options there are for compliance professionals to use it to help them in their jobs.

EN: Compliance professionals should view Twitter as one giant database of information provided by more than 200 million users. Compliance professionals on Twitter write posts (tweets) about the latest compliance news and hot topics, and ask each other questions about compliance concerns they may have. Also, for the latest compliance news, follow HCCA @hcca_news (www.twitter.com/hcca_news) and SCCE @SCCE (www.twitter.com/scce)

RS: Please tell us what benefits Facebook provides and what options there are for compliance professionals to use it to help them in their jobs.

EN: Facebook members should make an effort to "like" Facebook pages that provide news and information about compliance issues. When you "like" a page, you have access to all the information on that page. However, unlike a Facebook friend, the page cannot access your profile information, which allows you to maintain your privacy. "Like" HCCA at hcca-info.org/facebook and SCCE at corporatecompliance.org/facebook to connect with more than 7,000 professionals.

RS: Please tell us what benefits LinkedIn provides and what options there are for compliance professionals to use it to help them in their jobs.

EN LinkedIn is a social network that focuses on professional connections. With more than 100 million members, there is a good chance you can connect to the majority of your colleagues through their profile on LinkedIn. In addition, LinkedIn has a Groups feature, where members come together to discuss issues and share information. Simply go to the Groups section to search for groups related to your compliance industry. The HCCA Group (www.hcca-info.org/Linkedin) has more than 6,000 members who discuss health care compliance issues. The SCCE Group (www.corporatecompliance.org/Linkedin) has more than 4,300 members discussing corporate compliance issues from various industries. ComplianceEX is the largest compliance group on LinkedIn, and focuses largely on the financial side of compliance.

RS: Please tell us what benefits YouTube provides and what options there are for compliance professionals to use it to help them in their job.

EN: YouTube has video clips of speakers from compliance conferences. YouTube also has various short compliance videos that you may be able to incorporate into your training. Visit www.youtube.com/compliancevideos to see an example of some useful content for compliance professionals.

RS: Please tell us what benefits HCCAnet/SCCEnet provides and what options there are for compliance professionals to use it to help them in their job.

EN: The network allows members to join industry-related discussion groups, such as groups dedicated to chief compliance and ethics officers, the Foreign Corrupt Practices Act (FCPA), the Health Insurance Portability and Accountability Act (HIPAA), hospitals, finance, auditing and monitoring, and the list goes on. In addition, members can connect with other compliance professionals who work in their field or region. Members can also download documents that can assist in developing and maintaining their compliance program. Best of all, HCCAnet/SCCEnet is free for anybody to join, and now has more than 7,500 members.

RS: Please describe what "power users" of social media are doing to get the most out of social media for compliance professionals.

EN: Power users of social media embrace the idea that sharing their ideas and insight on compliance issues is the most effective way to advance the compliance profession as a whole. Thus, the power users I've seen on our social media sites provide consistent feedback and are open and willing to exchange ideas and provide resources to other members.

AT: I think the first thing that power users are doing is taking the time to understand the potential of social media. It provides enormous capabilities for people to connect, and not just on what movie they just saw or where they just had drinks. It allows people with similar interests to share both their passion and their wisdom.

If you haven't already, you should join groups around your professional interests on LinkedIn, and "like" pages for your personal and professional passions on Facebook, being aware of course, that you need to use some discretion, because a private passion quickly can become public information.

Just as important, you need to get a feel for why others are using social media to recognize that this is not something you can block. Whether you want them to or not, your workforce is going to spend a lot of time on these media.

The other thing to realize is that power users take advantage of social media to stay ahead of the curve. On Twitter we have a feed that provides the latest news stories on compliance. Our LinkedIn groups are filled with discussions and are great for networking. And, we're far from alone. Just about every specialty and sub-specialty has its own groups and feeds.

RS: You have conducted two surveys of the policy and procedures that companies have developed for dealing with employee use of social media. Tell us about the purpose of the surveys.

AT: Back in August 2009, it seemed like the compliance and ethics world was in a panic about social media. Out of nowhere, Facebook seemed to have gone from a vehicle for kids to complain about their schoolmates to a vehicle for adults to complain about their bosses.

So, we wanted to see what companies were doing and how bad the problem really was. What we found was that few had social media-specific policies and even fewer had actually had an incident at their company.

Our goal for the second phase of the research was primarily to see how things had changed. What we found is that companies are getting much more specific in their approach to social media. While our first survey showed that just 10% had a policy for employee social media usage outside of work, the recent survey showed that number had increased to 31%. That's a big jump.

We also found that companies are now discriminating among social network sites. Among our survey respondents, 47% reported that their company allows anyone to use LinkedIn at work, but only a bit more than 30% of employees are allowed to use Facebook or Twitter.

RS: Are some companies too restrictive? Are some companies not restrictive enough?

CONTINUED ON PAGE 33

Get Practical Guidance With:

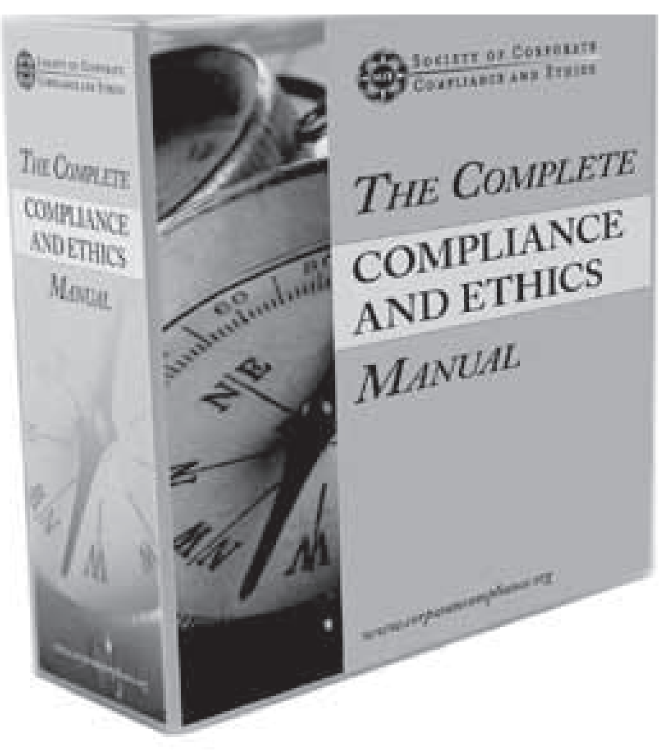
The Complete Compliance and Ethics Manual, Second Edition

What's in the New Edition:

- New material—400 additional pages of guidance—and more to come with the quarterly update system
- New structure includes greater focus on the global application of compliance and ethics as well as more guidance for specific risk areas such as conflicts of interest, government contracting, FCPA, and much more (see inside for table of contents)
- Subscription service allows continuous receipt of quarterly updates (the first four quarterly updates are free with purchase of manual)
- Data CD of entire book allows advanced keyword searches and offers clickable Web links for many additional resources

BOOK PRICE
AND ANNUAL SUBSCRIPTION RATE

$359 for SCCE members
$399 for non-members



From its introduction in 2004, *The Complete Compliance and Ethics Manual* has been serving SCCE's membership and the compliance and ethics industry by providing straightforward, practical advice and resources for the implementation and management of compliance and ethics programs.

With contributions from leading experts and practitioners, the new and improved edition of *The Complete Compliance and Ethics Manual* has evolved to provide more tools you need to efficiently and effectively improve your program.

AT: There's clearly a range of approaches out there. So, yes, inevitably some companies are going to find that their policies are either too restrictive or not restrictive enough. But, no matter where a company is today, they have to be prepared to change or review their policies regularly, maybe even several times a year.

As more and more organizations use social media for their own marketing, two things happen. One, more and more employees are going to need to have access to get their jobs done. Second, it gets harder and harder to justify blocking access. How do you tell your workforce, "We have a Twitter feed, and a Facebook page, but we don't trust you to use Facebook and Twitter"?

RS: Where are companies having trouble with their policies?

AT: I think the biggest challenge is in auditing and monitoring. Part of it is a reflection of technology. If someone posts something publicly, it's relatively easy to find. But, if someone posts in their status that their company stinks or their numbers for the quarters are great, that's close to impossible to find, if the employee is posting privately.

And, it's not like companies are working hard in the auditing and monitoring arena. We found that 48% of respondents rely on passive monitoring and another 18% didn't even know how their organization was monitoring social media.

RS: Where can people go to get sample policies and procedures for employee use of social media?

EN: A great site is http://socialmediagovernance.com/policies.php. I would also encourage users to access compliance-related social media sites and ask for policies and procedures from other users.

AT: Compliance Building has links to more than 200 of them at www.compliancebuilding.com/about/publications/social-media-policies/ ✳

Editor's note: This interview was recently conducted by Roy Snell with Eric Newman, Esq., CCEP, Social Media Manager, HCCA/SCCE and Adam Turteltaub, Vice President of Membership Development, HCCA/SCCE. Contact Roy by e-mail at roy.snell@corporatecompliance.org; Eric at eric.newman@corporatecompliance.org, and Adam at adam.turteltaub@corporatecompliance.org.

Whistleblower 3.0: Nuts and bolts of Dodd-Frank's whistleblower bounty provisions

By: Steven J. Pearlman, Esq. and Erik W. Weibust, Esq.

Score another victory for whistleblowers. On May 25, 2010, the Securities and Exchange Commission (SEC) released its final rules implementing the whistleblower bounty provision of the Dodd-Frank Act. As expected, the rules largely favor whistleblowers and were passed on a 3-2 party-line vote, with the SEC's two Republican commissioners voting in the minority. In short, the rules enable a whistleblower to obtain a bounty when he or she voluntarily provides the SEC with original information that leads to the successful enforcement of a federal court or administrative action, and the SEC obtains sanctions exceeding $1 million. The bounty can range from 10% to 30% of the sanctions awarded, which can be substantial (and, in any event, will be no less than $100,000). These rules add additional teeth to the already formidable Section 806 of the Sarbanes-Oxley Act (SOX), which protects whistleblowers from retaliation and provides a private cause of action, but does not offer direct monetary incentives to whistleblowers for merely reporting alleged misconduct.

It is important to understand the nuts and bolts of the SEC's rules in order to craft practical and effective anti-retaliation, internal reporting, and compliance programs and strategies. Indeed, it is imperative that public companies and their subsidiaries encourage and empower their legal, human resources, and compliance teams to work closely together to ensure that valid employee complaints are addressed properly in order to combat the obvious enticement of six- or seven-figure government-awarded bounties.

Nuts and bolts

For the Frank-Dodd bounty provision to be triggered, the SEC must first recover sanctions in excess of $1 million. For purposes of determining whether this threshold is met, the SEC may aggregate two or more smaller actions that "arise from the same nucleus of operative facts." As a practical matter, this will make bounties available in more cases and to more whistleblowers.

Once the $1 million threshold is met, to be eligible for a bounty whistleblowers must provide "original information" to the SEC. The rules define "original information" as information derived from the independent knowledge or analysis of the whistleblower that is not already known to the SEC from any other sources, and not exclusively derived from allegations made in a judicial or administrative hearing, government report, hearing, audit, or investigation, or from the news media. In addition, "original information" only includes information provided to the SEC for the first time after July 21, 2010 (the date Dodd-Frank was enacted). Although this definition may seem rather limiting, it leaves the door wide open for many types of information to be deemed "original," including most information that is gleaned internally from the whistleblower's position of employment or other relationship with the company.

Original information must derive from a whistleblower's "independent knowledge." The rules define "independent knowledge" as factual information in the whistleblower's possession that is not obtained from publicly available sources (e.g., corporate press releases and filings, media reports, and information on the Internet), and sources that, though not widely disseminated, are generally available to the public (e.g., court filings and documents obtained through Freedom of Information Act requests). This definition does not require that a whistleblower have direct, first-hand knowledge of potential violations. Rather, he or she may obtain actionable knowledge from observations, communications, and independent analysis of publicly available information.

That being said, independent knowledge does not include information that is:

- subject to the attorney-client privilege;
- learned through legal representation, even if not privileged (this includes in-house counsel), unless the disclosure has been authorized;
- secured through an engagement required under the securities laws by an independent public accountant if the information relates to a violation by the engagement client or the client's directors, officers, or other employees;
- obtained by officers, directors, trustees, or partners of an entity who are informed of allegations of misconduct, or who learn the information in connection with the entity's processes for identifying, reporting, and addressing possible violations of the law (such as through a help-line);
- obtained by employees whose principal duties involve Compliance or Internal Audit responsibilities or employees of outside firms retained to perform Compliance or Internal Audit work;
- obtained in a manner that is determined by a domestic court to violate applicable federal or state criminal law; or
- obtained from a person who is subject to the above exclusions, unless the information is not excluded from that person's use, or the whistleblower is providing information about possible violations involving that person.

There are, however, exceedingly broad exceptions to these limitations. In certain circumstances, for instance, Compliance and Internal Audit personnel, as well as public accountants, can be whistleblowers, such as when they believe that disclosure may prevent substantial injury to investors. It is difficult to imagine a situation where a whistleblower does not purport to have such a belief. An exception also exists where a whistleblower believes that the company is engaging in conduct that will impede the investigation. Likewise, Internal Audit personnel, public accountants and a potentially broad range of "other designated persons" may become whistleblowers after 120 days have elapsed since the whistleblower reported the information to her or his supervisor or the company's audit committee, chief legal officer, chief compliance officer, or since the whistleblower received the information, if the whistleblower received it under circumstances indicating that the foregoing individuals already are aware of the information. As a practical matter, this forces companies to address complaints quickly so as to avoid creating new potential whistleblowers.

A whistleblower also must have "voluntarily submitted" information to the SEC to obtain a bounty. Information is not deemed to have been voluntarily submitted where the whistleblower was required to report the information to the SEC. This requirement can arise by way of a pre-existing legal duty, a contractual duty, or a duty that arises out of a judicial or administrative order to report the information to the SEC. Likewise, information is not voluntarily submitted where it is done so pursuant to a request by the SEC that relates to the subject matter of the submission; in connection with an investigation, inspection, or examination by the Public Company Accounting Oversight Board (PCAOB) or any self-regulatory organization; or in connection with a government investigation.

Even if all of the requirements described above have been met,

CONTINUED ON PAGE 36

 CONTINUED FROM PAGE 35

whistleblowers who themselves have engaged in misconduct that is the subject of the SEC's action or a related action may be barred from recovering a bounty or limited in the amount they recover. For example, whistleblowers convicted of criminal violations related to the action for which they provided information are unconditionally barred from recovery. Otherwise, however, whistleblowers who have engaged in misconduct, but are not convicted of such, can recover bounties. In those cases, the SEC will not include sanctions that the whistleblower is ordered to pay, or that are ordered against an entity whose liability is based "substantially" on conduct that the whistleblower directed, planned or initiated, in determining whether the $1 million threshold has been met.

Finally, although the SEC's rules deal largely with bounties, they also protect whistleblowers who are not eligible for a bounty from retaliation, and prohibit companies from hindering whistleblowers' ability to communicate with the SEC. As such, companies cannot require employees to sign agreements requiring them to report complaints internally before going to the SEC. Notably, in contrast to the proposed rules, the final rules require whistleblowers to have a "reasonable belief" that the information they are providing relates to a possible securities law violation (or, where applicable, to a violation of the provisions in Section 806 of SOX) that has occurred, is ongoing, or is about to occur. The rules provide that "[t]he 'reasonable belief' standard requires that the employee hold a subjectively genuine belief that the information demonstrates a possible violation, and that this belief is one that a similarly situated employee might reasonably possess." Moreover, the SEC will consider the following in determining whether a whistleblower's belief is reasonable: whether the information provided to the SEC is specific, credible, and timely; whether it is related to a matter that is already under investigation by the SEC but significantly contributes to the investigation; and whether it was reported internally and then disclosed by the company (and satisfies either of the foregoing considerations).

In addition to the new rules, also on May 25, 2011, the United States Department of Labor's (DOL) Administrative Review Board (ARB) issued a dramatic decision in *Sylvester v. Parexel International LLC*[1] that significantly broadens the scope of what constitutes "protected activity" under Section 806 of SOX. Many believe it is no coincidence that this decision was issued on the same day as the SEC's new rules. The ARB's decision in Sylvester is important in several respects:

- It held that the heightened pleadings standards articulated by the Supreme Court in its recent *Twombly*[2] and *Iqbal*[3] decisions do not apply to SOX whistleblower claims initiated with the Occupational Safety and Health Administration (OSHA).
- It held that SOX Section 806 does not require a complainant to communicate the reasonableness of his or her belief that the company engaged in fraud to management or other authorities.
- It held that a complainant need not describe an "actual" violation of one of the categories of law in Section 806 of SOX to be protected (i.e., that an illegal act that had already taken place); but rather, a complaint concerning a violation of law that is about to be committed is protected, so long as the employee reasonably believes that it is likely to occur.
- It effectively overruled decisions holding that an employee's complaint must "definitively and specifically" relate to the categories of fraud or securities violations listed in Section 806.
- It held that protected conduct under SOX is not limited to disclosures that reflect fraud on shareholders.
- It held that a SOX whistleblower complainant need not establish the elements of criminal fraud to prevail on a Section 806 claim.

How the rules impact employers

The rules give employees an incentive to bypass the internal compliance mechanisms mandated by SOX, and complain directly to the SEC. Circumvention of internal compliance mechanisms will make it difficult for companies promptly to address the allegedly fraudulent conduct that forms the basis of the whistleblower's tip to the SEC. Moreover, there is a growing fear that the bounty provisions will actually encourage whistleblowers to let financial improprieties grow so that the size of the SEC's recovery and their corresponding bounty is higher.

As discussed in the companion article (see Whistleblower 3.0: Preparing for life under the new Dodd-Frank bounty rules, on page 38), there are proactive steps that companies should take to minimize the risk of whistleblower actions. Perhaps most important, employers should ensure that, where practicable, whistleblower claims are resolved internally, because employees now have a unique incentive (in the form of a bounty) to report perceived misconduct to third parties, such as the SEC, even before an employer can adequately address their concerns and remedy any problems. To that end, employers should provide multiple avenues through which employees can report perceived misconduct without fear of retaliation; promulgate appropriate codes of ethics and anti-retaliation policies; and train managers to be receptive and responsive to employee complaints. If and when an employee does report perceived misconduct, employers should take the matter seriously and promptly conduct a thorough investigation. Finally, if an investigation does uncover misconduct, companies should take all appropriate steps, with the assistance of experienced counsel, to remediate them as soon as possible so as to avoid further claims and limit potential sanctions.

The bottom line is that public companies need to foster a culture where their in-house employment and securities counsel, human resources professionals, and compliance teams are encouraged and empowered to work closely together to ensure that valid employee complaints are addressed properly and in a timely manner, and to avoid the appearance of retaliation resulting from employee complaints. On a broader scale, employers should adopt leadership models that foster a culture of open communication, integrity and accountability throughout the organization with an eye toward encouraging employees to raise complaints internally rather than to third parties. These steps serve to counter the lure of potential bounties. ✳

Notes:

1 *Sylvester v. Parexel International LLC*. Case No. 07-123, May 25, 2011. Available at http://www.dol.gov/arb/briefs/07-123/index.htm

2 *Bell Atlantic Corp v. Twombly*, 550 U.S. 544 (2007), which governs the pleading of factual content in federal court complaints.

3 *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (2009), which expressly applies to the pleading of each element, including knowledge and intent, in federal court.

Editor's note: Steven J. Pearlman is a Partner in Seyfarth Shaw's Labor & Employment department and is the Co-chair of the firm's national Sarbanes-Oxley Act (SOX) Whistleblower Team in Chicago. (www.seyfarth.com/SOX). He specializes in employment retaliation and securities and related corporate fraud-based litigation, defending management in high-profile SOX whistleblower cases brought by executives and managers. He may be contacted at SPearlman@seyfarth.com.

Erik W. Weibust is a Litigation Associate at Seyfarth Shaw LLP's Boston office. He is a member of the firm's national SOX Whistleblower team. He specializes in complex commercial litigation, including the representation of corporations and their officers and directors in securities, business, and employment-related litigation. He may be contacted at EWeibust@seyfarth.com.

Whistleblower 3.0: Preparing for life (and Compliance) under the new Dodd-Frank bounty rules

By Patrick Gnazzo and Donna Boehme

There's a new sheriff in town, and he's carrying a whistle. After more than 240 comment letters and 1,300 form letters, countless hearings, and a 3-2 vote by the Securities and Exchange Commission (SEC), the new Section 922 Dodd-Frank whistleblower bounty rules were finally published in May 2011. Not that whistleblower laws are anything new to Corporate America—both the False Claims Act and Sarbanes-Oxley created specific protections for insiders who report suspected misconduct. Yet the sheer scale of the potential financial incentives (i.e., 10%-30% of sanctions resulting from successful securities law prosecutions in excess of $1 million) should, without question, raise the bar for companies to seek out and correct wrongdoing quickly and effectively before employees feel the need to bypass their companies' internal reporting systems and take their concerns directly to the SEC's new whistleblower line. The question companies should be asking themselves in the world of Section 922 is, "Is our internal reporting system trusted by our employees and supported by our management, and if not, how do we enhance it so it is the preferred mechanism of choice for our employees?"

Some have dubbed the new rules a "game-changer," but in truth, nobody really knows where the moving parts will land, and what the SEC will actually do with the "tip a day" calls (and reportedly, higher quality tips) that it is receiving. What triage process will the agency use, what feedback will subject companies receive, and how will the investigation process be managed? And just as importantly, will the SEC treat "good" companies (the ones that have taken demonstrable steps to root out wrongdoing) from "bad" companies (the ones with no compliance program, or a program in name only). We will no doubt learn more about the SEC's process for dealing with the rising number of whistleblower calls over the coming months.

For now, however, it is clear that companies need to step up their game. From our perspective, the best response for companies is to conduct an honest assessment of their existing programs—internal hotlines and everything that supports them—and, if needed, to change the way that managers regard and support these internal mechanisms. And beyond just the reporting line, now is the time for companies to pay attention to the overall corporate culture, which will, in the end, drive whether employees will trust management enough to come forward—regardless of the promises or statements made in the code/policies, posters, or the CEO's annual letter.

Companies and management can take some concrete steps now, including:

- **Take a cold, hard look at your employee reporting line program.**

Job One should be ensuring that internal reporting mechanisms are in absolute tip-top shape, so as to assure employees who come forward that it is the company's intended goal to detect and prevent misconduct. Let's face it—too many hotline programs are run like a TV episode of "The Office." It really is time for companies to put some serious professional weight behind how they set up, resource, and implement these mechanisms.

Patrick Gnazzo

The hotline should have appropriate triage protocols, involving other relevant functions (e.g., whoever conducts or supports investigations), as appropriate. There should be clear, written investigation guidelines, and no one should be permitted to lead or support an investigation without being trained in these guidelines. For example, ex-law enforcement can be great assets to a compliance program, but they should be reminded via the guidelines that what works for the FBI may not be appropriate corporate protocol. Care should be taken to manage internal whistleblowers appropriately, identify and stamp out retaliation, and close cases on a timely basis. This process should be a coordinated effort among Compliance, Human Resources (HR), and the Legal departments. All of these aspects should be monitored and periodically audited. And above all, there should be a senior level, autonomous chief ethics and compliance officer (not some other officer with a fake "CECO" title tacked on), who has a seat at the table where important management decisions are being made, to oversee the integrity of the whistleblower program. More on that below.

- **Foster a culture of open communication**

A well-implemented internal reporting line should be only one part of an overall culture of open communication in the organization. There is not a "one size fits all" formula for an internal reporting system. The company's culture must be taken into consideration in determining whether third party and internal helplines, written communication systems (either on paper or electronic), and/or ombudsmen programs will be most effective, given the company's culture. And beyond these mechanisms, line management should foster an environment of open communication in which employees are encouraged to speak up and ask questions of their supervisors. It should be noted, however, that employees will quickly see through management's encouragement and support, if it is not meaningful and continuous. The CECO can strengthen that support by publishing the number of active investigations and general results, such as the number confirmed and the number of disciplinary actions taken as a result of the investigations. In addition, management's resolve in ensuring that the allegations investigated are

Donna Boehme

brought to the board of directors will go a long way in developing trust between the employees and management.

Some companies not only encourage a culture of open communication, they inform their employees that they have an obligation to report wrongdoing or risk disciplinary action themselves for remaining silent. When individuals understand that the company is serious about encouraging employees to speak up as an integral part of the company's culture, and that the employees will be praised rather than punished, potential wrongdoers will think twice before attempting to commit misconduct.

- **Monitor and root out retaliation**

Retaliation against employees who speak up is the surest way to keep them (and others who observe the retaliation) from

CONTINUED ON PAGE 40

 CONTINUED FROM PAGE 39

coming forward. Now, those same people can go directly to the SEC whistleblower line. Retaliation (in all its obvious and insidious, subtle forms) has always been a bad thing and a compliance program-killer, and now it can land a company in the SEC's crosshairs. This is a good time for Compliance, Legal, and HR to collaborate on meaningful ways to protect internal whistleblowers, and to ensure that misdirected disciplinary actions and performance improvement measures do not create additional retaliation risk. And while you are at it, be sure that everyone, including every layer of line management, is trained and understands what retaliation looks like. It is curious that many companies have never identified a single case of retaliation. Given human nature and the size of some of these companies, that's nearly an impossibility. Dodd-Frank is a good reason to demand that every layer of management adhere to a program of fostering open communication and break the dismal record of punishing the concerned and forthcoming employee because it "messes up our day."

- **Reward the behavior you want**

Paul Moore, the former head of risk at HBOS, PLC who turned whistleblower and testifier to the UK Parliament says "If you want someone to do X, pay them to do X." More and more companies that are serious about ethics and culture are tying compensation, performance evaluations, and promotions to compliance and ethical leadership metrics. You can train and preach ethics and compliance until the cows come home, but in the end, people will pay attention to how they are measured and compensated. So, if you want managers who walk the talk, support the hotline, uphold firm standards and don't retaliate, add an ethical and compliance leadership component into compensation or bonus calculation (or even better, establish a minimum score to even qualify for bonus). You can even have their supervisors, peers, and direct reports evaluate them against these metrics in a 360 degree review process.

- **Consider non-monetary recognition of ethical leadership**

We are aware that a number of companies are exploring internal "bounties" as a counter to Section 922, but no firm can really compete with the scale of Dodd-Frank. Moreover, an open advertisement that encourages employees to turn in misbehaving peers could create unintended consequences and send a mixed message.[1] That's not to rule out individual recognition (e.g. discretionary bonus) for an employee who has helped the company. But, there are plenty of ways to acknowledge, reward, applaud, and encourage ethical leadership in a non-monetary manner. In fact, surveys consistently confirm that when employees are asked what they most crave to be happy in the workplace, they rank recognition, trust, and engagement significantly higher than compensation.[2]

One of the simplest and most effective gestures we have seen is a letter and certificate from one CEO to each newly appointed compliance and ethics leader in the organization (i.e., senior business leaders who also acted as liaisons to the compliance program for their teams). Equally easy and effective is a recognition letter to any employee who shows compliance and ethics leadership.[3] Such non-financial gestures that acknowledge and reward the value of ethical leadership are not only free (and can be cascaded and imitated for free throughout the organization), they can have an enormous impact on company culture.

- **Document your program and commission an independent evaluation**

So this is good practice regardless of Dodd-Frank, right? But now, buried in a footnote[4] in the SEC rules and commentary, is a potentially significant nod to companies and CECOs who are serious about compliance. In that footnote commentary, the agency confirms that, although it will not be independently assessing whether a company's program is "effective," the SEC may in fact "consider information [it has] about the company's internal compliance programs" when deciding whether to refer a case back for initial investigation. It is unclear whether and to what extent the SEC may 'refer back' cases, but this suggests even more of a reason to ensure that a company's compliance program is meaningful and well-documented. Documents such as board resolutions that establish the compliance program mandate and escalation provisions, details about program structure and resources, reporting lines and organizational charts, functional mandate and other program elements might just change the complexion of the investigation, if a company finds itself responding to an SEC whistleblower complaint. Going one step further, commissioning an independent evaluation of a program by a qualified outside expert (who reports directly to the board without any filtering by management) goes a long way to demonstrate a company's commitment to making its program work. Just be sure to take action on the expert's recommendation.

- **Ask: Who's running the program? (The SEC may ask too.)**

In the Tenet Healthcare fraud case, Senator Charles Grassley took one look at the compliance program structure (i.e., general counsel also serving as chief compliance officer) and wrote "It doesn't take a pig farmer from Iowa to smell the stench of conflict in that arrangement."[5] Lynn Turner, former SEC chief accountant has also said publicly[6] that the CECO and whistleblower reporting line must not report to the general counsel, but directly to the Audit Committee, otherwise it is "worthless." These statements, when taken with a wealth of high profile settlement agreements, the 2010 amendments to the Federal Sentencing Guidelines that support a CECO with "direct reporting obligations" to the governing body,[7] and a rising chorus of voices calling for CECOs with independence and direct unfiltered access to the board suggest that companies interested in successful compliance programs should pay close attention to the qualifications and structuring of the CECO role. A strong empowered senior-level CECO with an independent budget, direct access to the board, and other resources is the first step to building an effective program that works as intended.[8] As referenced above, the SEC has indicated that it may take note of information it has on a company's compliance program. If there was a single leading indicator we would recommend to the SEC, it would be the creation of a robust CECO role, the one individual tasked with leading and overseeing the program (and the reporting line).

- **Clarify the role of Legal vs. Compliance**

One of the trickier areas to get right is the role of the general counsel with respect to internal compliance investigations. Lack of clarity on the role of Legal vs. Compliance undermines the independence and effectiveness of the compliance program and the company's ability to detect and prevent wrongdoing. This is because the two functions have different, but equally important, mandates: the general counsel has an obligation to use all legal means to protect the corporation (unless management waives that duty), while the CECO leads a program to detect and prevent misconduct and to support a culture of integrity throughout the organization. In a perfect world, Compliance oversees internal investigations, working closely with Legal as a partner and subject matter expert in a number of key risk areas. However, as spectacularly demonstrated in a number of recent high-profile corporate fraud cases, this dynamic can be skewed where the general counsel is the CECO, or the CECO reports to the general counsel.[9] The board of directors, the CEO, the general counsel, and the CECO must be in sync in understanding that the misconduct must be dealt with, the wrongdoers must be disciplined, and the whistleblower not only protected but praised for doing the right thing.

Companies in the age of Whistleblower 3.0 would be wise to put themselves in the place of an

CONTINUED ON PAGE 42

 CONTINUED FROM PAGE 41

employee who has just witnessed serious misconduct. Ask yourself:

- "What messages, overt and subtle, has my line manager given me about speaking up?"
- "If I do report, will anything actually be done?"
- "Do I feel safe speaking to my supervisor, Compliance, Legal, or HR?"
- "Can I really report anonymously?"
- "Do I feel positively about how whistleblowers have been treated around here?"
- "Would my peers support me if they found out?"
- "Is the CECO and compliance program really independent enough to handle my report?"

Any company where the answer to one or more of these questions is "No" really has zero standing to complain about employees who go directly to the SEC. It's going to happen, and for good and predictable reasons.

Make no mistake: reporting a concern is hard, and requires courage, encouragement, and an organizational culture that supports speaking up and dispels cynicism. In the 40+ combined years that the authors have practiced in the field, we have never once heard of an employee's reason for remaining silent to be "because they didn't offer me enough money." Becoming a whistleblower is almost never about just money, unless it's overcoming a fear of losing one's job. In fact, surveys show that the most common reason that employees report concerns is "outrage." That's why—even given the potentially large Dodd-Frank rewards at stake—those who are focusing solely on the "bounty hunter" phenomenon may well be proved short-sighted. The decision to come forward involves a complex mix of apprehension and courage, team culture and engagement, personal situation and responsibility, company loyalty, and a host of other individual and organizational factors. The primary goal should be to create an environment where, given all these considerations, employees make the natural choice to report internally. Companies that are serious about a culture of open communication, compliance, and ethics must support internal reporting programs that will actually be trusted and used as an alternative to external whistleblowing. For most of our companies, that culture is currently weak at best, requiring solid management commitment, resources, and a CECO who has an appropriate degree of autonomy and direct access to the board to make open communication programs effective. ✳

Notes:

1 Eleanor Bloxham: "How to Encourage the Right Kind of Whistleblower" *Fortune* online, June 15, 2011. (Citing study by University of San Diego law professor Orly Lobel , suggesting that, for women in the workplace, the offer of small monetary payments may actually crowd out" their desire to report wrongdoing.) Available at http://management.fortune.cnn.com/2011/06/15/how-to-encourage-the-right-kind-of-whistleblowers/

2 Bob Nelson: ***1001 Ways to Reward Your Employees.*** Workman Publishing Company, Inc., May 2005.

3 Joseph E. Murphy: ***501 Ideas for Your Compliance and Ethics Program: Lessons from 30 years of practice.*** Society of Corporate Compliance and Ethics, 2008.

4 "Implementation of the Whistleblower Provisions of Section 21F of the Securities Exchange Act of 1934. Release No. 34-64545, Fn 274, p. 125. Available at http://www.sec.gov/rules/final/2011/34-64545.pdf

5 September 5, 2003 Letter from Sen. Charles Grassley to Mr. Trevor Fetter, Acting CEO, Tenet Healthcare Corporation. Available at http://grassley.senate.gov/releases/2003/p03r09-08.htm

6 Comments of former SEC Chief Accountant Lynn Turner at a 2008 PLI Compliance and Ethics Conference.

7 See law firm memorandum summarizing the 2010 Federal Sentencing Guidelines amendments on "direct reporting obligation." Available at http://www.skadden.com/Index.cfm?contentID=51&itemID=2074

8 See 2009 RAND report "Perspectives of Chief Ethics and Compliance Officers on the Detection and Prevention of Corporate Misdeeds: What the Policy Community Should Know." Available at http://www.rand.org/pubs/conf_proceedings/2009/RAND_CF258.pdf

9 For example, the 2009 Pfizer Corporate Integrity Agreement required that the chief compliance officer "shall not be, and shall not be subordinate to, the General Counsel or the Chief Financial Officer." Available at http://oig.hhs.gov/fraud/cia/agreements/pfizer_inc_08312009.pdf
See also, Tenet Healthcare and Bayer corporate integrity agreements. Available at http://oig.hhs.gov/fraud/cia/agreements/TenetCIAFinal.pdf; http://oig.hhs.gov/fraud/cia/agreements/fully_executed_bayer_cia_112508.pdf

Editor's note: Patrick Gnazzo is Principal, Better Business Practices LLC in McLean, Virginia and former chief compliance officer at two leading multinationals. He specializes in evaluating and developing compliance and ethics programs. Pat may be contacted by e-mail at patrick.gnazzo@gmail.com or by telephone at 703/531-9091.

Donna Boehme is Principal, Compliance Strategists LLC in New Providence, New Jersey and former chief compliance officer at two leading multinationals. She advises a wide spectrum of private, public, governmental, academic and nonprofit entities in compliance and ethics solutions. Donna may be contacted by e-mail at dboehme@compliancestrategists.com.

Foxes and henhouses: The importance of independent counsel

DAN DUNNE

By Dan Dunne, JD

Two significant recent events train the spotlight on corporate whistleblowers. On May 25, the Securities and Exchange Commission released its proposed final rules under the Dodd Frank Act on whistleblowers who report possible violations of securities laws. In its final rules, the Commission rejected the most important criticisms filed by public companies, including the widespread concern that the rules would gut internal compliance programs. As if on cue, on the same day, the US Department of Labor's Administrative Review Board reversed an administrative law judge's dismissal of whistleblower claims under the Sarbanes Oxley Act, and adopted liberal standards that will favor whistleblowers pursuing retaliation claims. These two events portend the road ahead for corporations confronted with whistleblowers, and highlight the need for corporations to ensure that their policies and procedures deal lawfully and effectively with whistleblower complaints.

A critical element of an effective whistleblower response is fair and objective evaluation. The need to investigate whistleblower complaints objectively dictates, in many cases, who should investigate and who should supervise the investigation. Think foxes and henhouses. It is equally important to avoid any conduct that even suggests retaliation. When investigating significant whistleblower complaints, the only reliable way to achieve objectivity and avoid the appearance of retaliation is for the company—typically a committee of the board—to retain truly independent outside counsel.

Why does the independence of counsel matter? To answer this question, you must first understand that the intended audience for the conclusions drawn from an investigation of a whistleblower complaint is often not the corporation, but outsiders—federal law enforcement agencies, judges, and potential plaintiffs in civil litigation. Although a corporation may have well-justified faith in the abilities of its regular corporate counsel (or else they wouldn't be regular counsel), it is not really the corporation's view that counts. In any investigation that matters—and this includes every investigation that asks a federal agency, judge, jury or third party to rely on its findings—the single most important factor in gaining such third-party trust will be counsel's independence. Almost by definition, at the start of any objective investigation you will not know the conclusions that will ultimately be drawn. It follows, then, that all investigations of serious whistleblower claims "matter" and should be designed for third-party consumption from the outset.

Retaining independent counsel

At least three fundamentally significant factors should cause a corporation subject to the whistleblower provisions of Dodd-Frank to retain independent counsel for internal investigations of most serious whistleblower complaints.

First, for a corporate ethics policy to be effective, employees must have confidence that their complaints are handled in confidence, treated seriously and objectively, and that they will not face retaliation. Even if the corporate body that supervises an investigation is considered beyond reproach, if that body hires management's lawyers, will employees have confidence that management won't be briefed or tipped and that their identity will remain confidential? And what if the whistleblower has actually worked directly with that firm and its lawyers in performing his or her duties? While the law firm might have the best intentions in terms of maintaining confidentiality, the appearances may be more important than their actions. Whistleblowers who conclude that their complaints are not fairly and objectively investigated are more likely to report to law enforcement agencies like the Securities and Exchange Commission (SEC). And if litigation erupts, these appearances can constitute evidence that could lead courts or juries to draw various negative inferences, regardless of the underlying truth of the matter.

To appreciate how pervasive this problem can be, consider that at the start of almost every interview with company employees, the investigating lawyer will begin by giving an Upjohn warning (also known as a corporate Miranda speech), advising that the employee is not the firm's client, that the corporation is the client, and that the corporation may decide to divulge the information communicated by the employee if it is in the corporation's best interests. This awkward beginning may cause employees to be confused or uncertain about confidentiality, and justifiably suspicious that their statements could be relayed to management, to their detriment. Some employees will equate this corporate Miranda to legal cautions with which they are far more familiar: "What you say can and will be used against you." The self-preservation instincts aroused by the corporate Miranda instruction are real, and regaining trust that management's lawyers will respect their confidentiality after hearing this instruction is a challenge. Appropriate reassurances of confidentiality from independent counsel are likely to be better received than those from interviewers perceived as "management's lawyers."

Second, if regular outside counsel conduct an investigation that comes to touch on their own prior advice or legal work, a plethora of loyalty and privilege problems can arise. The first problem is that the lawyers' powerful instincts for self-preservation (i.e., avoiding malpractice claims) may result in prejudice to the client, if the client does not receive from corporate counsel complete information about corporate counsels' prior advice.

Unrelated to this problem but equally significant, if there is a later decision to waive the attorney-client privilege in the investigation, a "subject matter" waiver could jeopardize other communications with the same law firm that are on the same subject matter but did not occur in the investigation. For example, if SEC disclosure counsel advised management or the directors about executive compensation matters, retaining the same firm to investigate allegations of improprieties because they "have a leg up" substantially increases the risks for waiver of the privilege on all of the firm's prior advice about compensation. Ring-fencing earlier corporate advice from later investigatory advice is more difficult when the same firm is involved in both phases, and lines become blurred. The law firm and the client might not even recognize that there is a relationship between the earlier advice and the later investigation at the time the investigation starts. Corporate decisions about whether and how to waive privileges in communications with law enforcement agencies are fraught with complexity and grave risks, but this scenario—facing the risk of a broad waiver of privilege over sensitive communications with the firm's outside counsel—may actually prevent the client from having

CONTINUED ON PAGE 46

 CONTINUED FROM PAGE 45

a meaningful choice whether to waive the privilege as to information that it might otherwise wish to disclose to government lawyers.

On top of these problems, the risk that other privileged communications related to the same subject matter will only be discovered or recognized after the investigation is well under way may result in a forced withdrawal of legal counsel that (1) consumes large amounts of board time and attention; (2) leaves the client with the unwelcome prospect of paying a new firm to re-start the investigation from scratch; and (3) jeopardizes relations with or commitments to the SEC, the Department of Justice (DOJ), or other law enforcement agencies about the time line to complete and report on the investigation. Worse still, the involvement of regular corporate counsel might taint the entire investigation in the eyes of lawyers for the government, with potentially irremediable consequences for future enforcement actions, whistleblower claims, or shareholder lawsuits.

The third major issue involves relations with law enforcement. In a high percentage of situations, it is necessary or desirable to report to law enforcement agencies on the results of the investigation. This is a critical task, and if the report of investigation is relatively favorable to the company and management, one of the questions any government lawyer will need to ask is whether the internal investigation was a "whitewash." One common prejudice often voiced by lawyers in federal enforcement is that any investigation conducted by regular corporate counsel cannot be objective and cannot be relied on for law enforcement decisions. When an agency such as the SEC or DOJ cannot rely on the company's own internal investigation, it necessarily either conducts its own, or expands the scope of its own investigation. This can be bad enough, but the agency may also proceed with an unnecessarily jaundiced view of the corporation, and perhaps with suspicions of a "cover up." Were the files cleaned up? Were witnesses influenced? Were the facts massaged and stories coordinated? Having the agencies preoccupied with these kinds of questions is not helpful to a quick, fair, and optimum resolution, especially if the agency must also consider potential obstruction of justice issues. Getting off on the wrong foot with enforcement authorities may make all the difference, and obviously, any justification of saving legal expenses by using existing counsel already familiar with the company would be criticized heavily in hindsight should these circumstances come to pass.

The appearance of bias

In-house corporate lawyers may be unfamiliar with these complications, and need to turn to outside counsel for guidance. Will your regular corporate outside counsel give you this same advice? Excellent lawyers fully devoted to the best interests of their clients will obviously do so when appropriate. In some situations, however, current counsel may hesitate. Partners in law firms have strong incentives to increase their billing credits and may find ways to rationalize to themselves and their clients why their firm should handle an investigation, notwithstanding these complications, especially if outside corporate counsel are unfamiliar with these land mines, which is true of many corporate lawyers who are not white collar litigators. And in an increasingly competitive global legal market, some regular outside counsel can also behave like jealous spouses, living in fear that if they introduce their best clients to another law firm they might lose their client.

Corporations should take these biases and shortcomings into consideration in evaluating any advice from outside counsel offering their own firm's services for internal investigations. They should seek input and guidance from other counsel experienced in internal investigations, which is readily available. Corporations faced with investigations of whistleblower complaints might also consider the famous words of Donald Rumsfeld that in addition to "known unknowns," there are also "unknown unknowns."

At the outset of a fast-moving internal investigation, it may not be possible to know all of the contingencies, conflicts, and relationships that will come within the scope of the investigation, and it is hubris to think otherwise.

The best approach is almost always a cautious prophylactic approach—to choose a strategy that minimizes the potential for these conflicts to occur. In most circumstances, this will require retention of independent outside counsel to assist in responding to whistleblower complaints. In short, to be independent, a law firm should not provide regular advice or services to the corporation, and its lawyers should not have personal relationships with officers or directors that might give even the appearance of bias. Again, objectivity is the goal, and even a slight appearance of bias or favoritism can be more damning than the reality.

Disadvantages

Are there disadvantages to retaining independent counsel? There can be. One disadvantage is that independent counsel may lack familiarity with the company, and may need to incur additional expense to get up to speed. Although familiarity may be helpful, this problem is less than meets the eye. Gaining adequate familiarity with the area to be investigated is usually a manageable task, and in order to be truly objective, the investigation must be conducted without preconceived ideas or blinders. Additionally, investigating counsel may interview and obtain the fruits of the corporate counsels' existing knowledge. It is also possible to design internal investigations that are either scalable or phased, and thus expand or contract in size and scope as circumstances and developing information dictate.

A second perceived disadvantage may be that management is less comfortable with investigating lawyers with whom they are not familiar. Here again, query whether having management who are comfortable with lawyers they know well—and to whom the lawyers are beholden—is even a desirable objective. Think foxes and henhouses, accented with divided lawyer loyalties.

Whistleblower complaints are dangerous. Once the tag "whistleblower" attaches to an employee, even a misinformed or misguided employee, the consequences of mishandling the complaint can range from serious to catastrophic. Whether a complaint is handled properly or improperly is in large measure in the eyes of the whistleblower, and counsels' conduct of any investigation is crucial. When a mishandled complaint turns into a whistleblower lawsuit, they can be extraordinarily difficult to defend. It is very hard to attack the whistleblower's claims without appearing to attack the whistleblower, especially when the whistleblower is opportunistic. Judges and juries are highly protective of all employees who wear the mantle of the whistleblower, not to mention Congress and federal whistleblower laws. Think David and Goliath, but David has an army of lawyers orchestrating a media circus, and David has a mutual defense treaty with the law enforcement agencies of the United States of America.

Truly independent counsel

The cost of defending government enforcement actions, whistleblower claims, and shareholder lawsuits can exceed the expense of an objective investigation by orders of magnitudes. The trouble is, a corporation may be unable to predict in advance which whistleblower complaints pose serious threats to the corporation, and the consequences of guessing wrong may lead to disaster. The only recognized tonic is to address all complaints objectively, and where a complaint is determined to involve serious allegations, to ensure the objectivity of the investigation by retaining truly independent counsel who does not have disabling relationships with management.

There may be situations where retaining regular corporate counsel's firm would be appropriate to review a whistleblower claim, but they would be the exception rather than the rule, and may often be

CONTINUED ON PAGE 49

 CONTINUED FROM PAGE 47

limited to an initial review to determine whether a more intensive investigation is warranted. Generally, caution is the better part of valor, and independence of counsel can vaccinate a company against many of the unforeseen ills that befall investigations of whistleblower complaints. ✳

Editor's note: Dan Dunne is a litigation partner at Orrick Herrington & Sutcliffe, LLP in Seattle, Washington. He specializes in corporate governance and securities litigation, including internal investigations. Dan may be contacted by e-mail at ddunne@orrick.com.

BE SURE TO GET YOUR CCEP CEUS

Complete the *Compliance & Ethics Professional* quiz related to the articles below:

Managing conflicts of interest: The basics—By Meghan K. Daniels, page 10

Whistleblower 3.0: Nuts and bolts of Dodd-Frank's whistleblower bounty provisions—By Steven J. Pearlman and Erik W. Weibust, page 34

Foxes and henhoues: The importance of independent counsel—By Dan Dunne, page 44

CEU Credit Procedure

Visit www.corporatecompliance.org/quiz. Select a quiz, fill in your contact information, and answer the questions. The online quiz is self-scoring and you will see your results almost immediately. Or, you may FAX or MAIL the completed quiz to CCB at SCCE. Questions? Please call CCB at +1 952 933 4977 or 888 277 4977.

Please note that credit will be given only for quizzes received before the expiration date indicated on the quiz.

Lessons From OZ

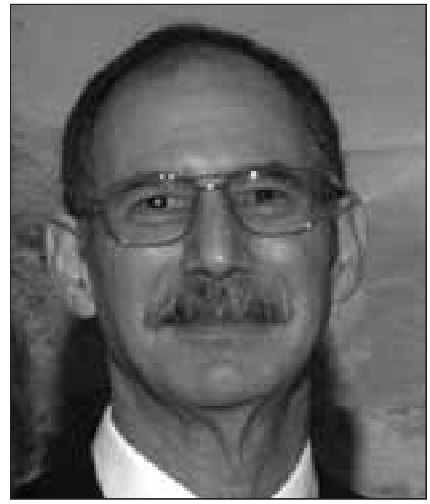
By Frank J. Navran

We live in challenging times. Although little of what we are facing is unprecedented in history, for most of us, this is the first time in our lives that we have to deal with the combination of economic, political, social, and organizational turmoil on this scale and for this duration. For most of us, these are uncharted waters. We are responsible for the management of the ethics component of our organization's culture in times of extreme challenges. But we are not the first, and are certainly not the only ones, facing complex and persistent obstacles that threaten our view of the future.

It may be useful to see if we can learn by the examples of others who have successfully navigated similarly challenging circumstances. Perhaps there are lessons they can teach us.

My favorite example of survival among unprecedented challenges is not found in the business literature. Rather it is contained in The Wizard of Oz, first published circa 1900 and later popularized by the 1939 "post-Depression era" film classic of the same name. We all know the story. Dorothy was carried from Kansas to Oz by a tornado—a powerful, unpredictable and uncontrollable force of nature. It landed her in a place where everything was different, a place, frankly, where she didn't want to be and from which she desperately wanted to escape. She longed for the safety and security of Kansas where events, while challenging, were at least familiar.

Many people today see the world changing around them and feel a similar sense of displacement. They recall a kinder, gentler, more stable, not-too-distant past. Today's world feels a bit like Oz. Technology changes faster than we can keep up. The world map is full of names and places that we never learned about in school. Our economy is troubled. Our political beliefs are challenged by the continuing redefinition of our friends and foes—foreign and domestic. Our economy has been crippled by the unparalleled greed of a few and the indifference and/or ineffectiveness of many. Consequently, our workplace is experiencing downsizing, restructuring, and uncertainty. Change has become so regular that many of us feel as though any semblance of control over our lives is just beyond our fingertips—just out of reach.



FRANK J. NAVRAN

Dorothy could blame the tornado for taking her away and the Wicked Witch of the West for blocking her return. Wanting to blame something or someone for the undesired events in our lives is a natural response.

So, who is to blame for all the bad things happening to us?

It was a tornado that brought Dorothy to Oz. But, as is often the case, knowing the cause of a problem will not necessarily lead you to the solution. After landing in Oz, Dorothy needed to focus on reaching the Wizard, all the while coping with the efforts of the Wicked Witch of the West, whose sister was killed when Dorothy's house landed in Oz. It was the Witch, not the tornado, that was the villain of this story.

When facing severe challenges, it is in our psychology to search for someone to blame for our situation. Absent a villain, we have to take personal responsibility, and that is not usually our first choice. In our search for a villain, we often settle on a vague collective sense of those we imagine to have been in control: the ubiquitous "they." Surely, they did it. In organizational parlance, "they" typically translates to "leadership"—those at a higher level than ourselves who are to blame. They were in charge, and since this happened on their watch, then surely this is their fault. But, how and why could our leaders have done all this to us?

In trying to figure out the hows and whys, some take their cue from the Scarecrow's lament. **If only they had a brain.** The chaos we are experiencing must result from leaderships' incompetence. They should have anticipated and prepared us for the potentiality and severity of all that is new. After all, they were in charge. They should have known. They should have seen it coming.

Some take a cue from the Tin Woodsman. **If only they had a heart.** The negative consequences of all that has changed can be blamed on the leaders who substituted personal ambition and greed for moderation and compassion. If they cared about us (employees, shareholders, consumers…) and the people like us, they would never have led us down this path. They would have worked harder to preserve what was good for all those to whom they owed an obligation or had some responsibility.

The Cowardly Lion's lament serves others. **If only they had courage.** They could have stood up to whatever forces were challenging them and said, "No." If they had mustered the courage to do the right thing, whatever that might have been, we wouldn't be in this mess.

But notice, it is always "they" who are to blame. It is never "us." It is never our fault.

Returning to Kansas

In Oz, Dorothy just wants to find the Wizard so he can tell her how to get back to Kansas, where everything was the way it was supposed to be. She wants to be magically transported back to the old, comfortable reality. And in the storybook land of Hollywood in the 1930s, that is exactly what happens.

As the victims and survivors of unforeseen and, for some, devastating change in our collective circumstances, we also want to be magically transported back to the glory days of just a few years ago. We were promised there could never be another "Great Depression." We were told that "consumerism" was good. Consumer spending, along with ongoing investment in the futures of proven and emerging organizations, were the engines that would drive our economy. Our debts would be absolved by the rising value of our holdings. We were a great world power and our economy powered the globe.

Now, we want to be taken back to a time when change moved at a manageable pace, where we could plan a future for our children and ourselves. We wish for a time and place where there are fewer surprises. We need to find a Wizard!

Well, there is no Wizard. There are no ruby slippers. And there is no real value in focusing on whom to blame. It doesn't do a lot of good to curse the tornado. It is simply the natural consequence of a foreseeable set of circumstances. It is what happens when certain preconditions are met. And the various witches, while evil, were largely operating within the letter, if not the spirit, of the applicable laws and regulations.

But, circumstances changed. Our financial house, built on a shaky foundation, eventually fell. We all face a new reality. Everything changed, seemingly overnight. And recovery is a long, slow, and uncertain process. What is certain is that, like Dorothy's tornado, change is an unpredictable and unstoppable force of nature and we are at its mercy.

But, what about our leaders? This is all their fault. Why can't we blame them?

With very few, and notable, exceptions (e.g., Bernie Madoff and his ilk), our leaders are not evil villains. They are people, most of

CONTINUED ON PAGE 52

 CONTINUED FROM PAGE 51

whom were simply doing the best they could with what they knew and what they had to work with, based on what had worked before. In that regard, they are not so different from us. They bought into the same myths and are living with similar consequences.

But aren't they incompetent? Some are. And so are many of us, sticking to time-honored practices and beliefs, long after they have lost their utility. We are choosing to continue doing what we knew was no longer working because change is so hard. We are letting momentum carry us along, rather than seeking and embracing what is good about the "new."

But, aren't they self-centered? Some are. And so are many of us, insisting on preserving what served our needs in the past rather than focusing on newer, creative solutions for the future of all.

But aren't they cowardly, heartless, all of those things we desperately wish them to be, so we can blame them for our hard times? Some are. And, by not taking personal responsibility for what happens next, so are many of us.

Taking Charge

Some in Oz may have been mindless, heartless, or cowardly. Others might have been particularly intelligent, compassionate, or courageous. Ultimately, that mattered less to Dorothy and her success than Dorothy herself. Here she was, transported against her will, a stranger in this alien and sometimes-hostile environment. Like many of us in the face of overwhelming change, she began her adventures bewildered, uncertain, fearful, and worried. How was it that she survived? What can she teach us? After all, The Wizard of Oz is a "morality play" —a Depression-era story with a lesson about how we ought to live our lives.

There were four keys to Dorothy's success:

Goals. She knew what she was trying to accomplish. She had a clear and specific set of short-term and long-term goals. Follow the Yellow Brick Road. Get to the Emerald City. See the Wizard. Kill the Wicked Witch. Look after Toto. Return to Kansas.

Persistence. Dorothy never lost sight of those goals despite the many short-term distractions Oz held in store. Whether it was sleepy poppies, flying monkeys, a stubborn gatekeeper, or a fraud of a Wizard, Dorothy never gave up.

Adaptation. She continually changed her tactics to meet the challenges she found in Oz. Her commitment never wavered. While her short-term tactics creatively reflected her immediate reality, her long-term goal stayed essentially unchanged. Go home!

Responsibility. Dorothy came to realize she could not depend on anyone else to solve her problems. The Wizard and the Good Witch tried to help in whatever ways they could. But the ultimate responsibility for attaining success was hers. The leaders were not capable of getting her what she wanted. They created the context. Success was a function of her ability to creatively and positively negotiate a path through all that was changing around her.

Our reality

Unlike the case with Dorothy, the challenges we face are not a dream. Neither are the lessons of goals, persistence, adaptation, and personal responsibility. We need to move beyond assigning blame to the brainless, heartless, and cowardly who got us into this mess. We need to get on with the work of attaining success. We need to set goals and to persist in achieving those goals. We need to find new ways of succeeding when the old ways fail. But most of all, we need to understand that our personal and collective success is our responsibility.

Though "they" make decisions that affect us, ultimately it is "we" who must deal with the situations that result. The lesson of Oz is that if anyone has control, it is we who have it. We can set our own goals and follow our own paths. We can fight our own battles. While we cannot be assured of the success of our actions, we can be certain that accepting responsibility for those actions is the only path that leads us out of Oz.

As ethics professionals, that translates to five key challenges:

Compliance. We all start with compliance. That is our bedrock, the foundation upon which all else rests. If we are not "in compliance," we have failed. That is also the easiest case to make: Do X or pay a fine and/or go to jail. But our challenge is to keep compliance in context. While it is the basis upon which we build ethics success for the organization and its leaders, an ethical culture is the ultimate goal. Compliance is a necessary but insufficient prerequisite.

Legitimacy. We have to continuously fight to defend the legitimacy of the investment needed to build and sustain an ethical culture. We cannot settle on satisfying Federal Sentencing Guidelines and their promise of reduced exposure, if we want an organizational culture that can prosper in challenging times. Compliance is not enough. Avoiding fines and reducing exposure is the entrance fee—the cover change—but not the definition of success.

Economics. We have to continuously find new, legitimate rationales for investing in what many see as an "intangible" in a time when resources are scarce and the focus is shifting to short- and shorter-term objectives for so many. Yes, there are false economies that seem attractive, but it is our responsibility to find the compelling arguments to sustain progress towards the actual, sustainable goal of an ethical culture.

Focus. We have to define the goal and keep our eyes on that target. Interim goals are important milestones, but we need to be cautious that we, and those on whom we rely, do not confuse crossing Ts and dotting Is with "success." The goal is an ethical organizational culture, based on a shared set of values, where everyone understands that each and every decision needs to be consistent with the standards of right, fair, and good, as well as in conformance with all of the applicable rules and regulations.

Context. We have to deal with the contexts in which we operate. Global economics, political realities, competition, stakeholders, shareholders, suppliers… and the list goes on. We also need to remember that, as leaders, we create the context for the tens, hundreds, or thousands we employ. We create the culture that defines what is right, fair, and good in our organization—what is expected and what will be accepted.

We are neither the tornado nor the Wizard. We are the designated leaders who can empower the inner "Dorothy" in all of those in our organization. We can also help those in the boardroom and the C-suite in their efforts to create and sustain an ethical context within which every employee, at every level, individually and collectively, can earn their own personal success by contributing to our mutual success.

Especially when the world starts to feel a bit like Oz, we need be the ones who understand the fundamental reality. Our commitment to an organizational culture founded on a shared set of ethical values provides stability and focus; and that is what keeps us on the Yellow Brick Road to our goals. ✳

Editor's Note: Frank J. Navran is the Founder and Principal Consultant of Navran Associates. Frank has worked with clients in more than twenty countries, reducing their risk of ethics and/or compliance failures and contributing to their success in developing and sustaining strong ethical cultures. Frank has authored five books and more than two hundred articles and book chapters. He may be contacted by e-mail at frank@navran.com, or for more information, www.navran.com.

Welcome to SCCE

The Society of Corporate Compliance and Ethics welcomes the following new members and organizations. All member contact information is available on the SCCE website, www.corporatecompliance.org, in the Members-Only section.

ARGENTINA
- Ana Corbellini, Johnson & Johnson
- Javier Lozada, Philips Argentina SA

AUSTRIA
- Darina Heger, Austria Tabak GmbH (JTI)

AZERBAIJAN
- Azer T. Gasimov, BP Exploration Caspian Sea LTD

BELGIUM
- Karl Boonen, Johnson & Johnson
- Guy De Witte, Johnson & Johnson
- Alan Greenwood, Dow Corning Corp
- Laura Harth, Patronale Life NV
- Vincent Nys, Johnson & Johnson

BRAZIL
- Eunice Alcantara, Bristol Myers Squibb
- Vitor Calazano Baroni, Mitsui Cas E Energia Do Brazil LTDA
- Sergio A. Pinto, Johnson & Johnson
- Maristela Rodrigues, Affinia Automotiva Ltda
- Andre Souza, Johnson & Johnson
- Izumi Takeno, Mitsui Gas E Energia Do Brasil Ltda
- Celso Viana, Mitsui Gas E Energia Do Brasil Ltda.

ALBERTA, CANADA
- Patricia McLeod, AltaLink

QUEBEC, CANADA
- Alain Falardeau, Noveko International Inc.

COLOMBIA
- Hector Bedoya, Johnson & Johnson

CYPRUS
- Constantinos Loizides, Piraeus Bank (Cyprus) Ltd

DENMARK
- Rasmus Juul Joergensen, Dong Energy

FINLAND
- Minna Kuusio, Pohjola Insurance Ltd

HONG KONG
- Ivan Yuen, Cathay Pacific Airways

ITALY
- Diego Ciccarelli, Johnson & Johnson

JAMAICA
- Alveta Knight, University of Technology
- Ashlyn Malcolm, Petroleum Corporation of Jamaica
- Jennifer Simpson-James, Petroleum Corporation of Jamaica

JAPAN
- Edmond Courtroul

MALAYSIA
- Teoh Poh Khim, JTI Business Services (Asia) Sdn Bhd

MONTENEGRO
- Ranka Jovanovic, Railway Transport of Montonegro
- Zorica Soc, Railway Transport of Montenegro

PERU
- Enrique Dedekind, Banco De Credito Del Peru

POLAND
- Katarzyna Tarnowska, Wix-Filtron

ROMANIA
- Melina Tataru, Romtelecom

RUSSIA
- Anatoly Yakorev, Center for Business Ethics & Corporate Governance

SINGAPORE
- Kevin Lam, McDermott Asia Pacific Pte Ltd

SLOVINIA
- Aleksandra Bercic, Zavarovalnica Maribor Insurance Company
- Maja Javorsek, Triglav Insurance Company Ltd

SWEDEN
- Charlotta Lekman, If P&C Insurance Ltd
- Ann Lundberg Wickham, If P&C Insurance Ltd

SWITZERLAND
- Claudia Italia, Johnson & Johnson
- Patrick Kempenaer, Johnson & Johnson

UNITED KINGDOM
- Ruth N. Steinholtz, AreteWork LLP
- Sharon Frank, Johnson & Johnson

ALABAMA
- Michael Bryan, University of Alabama in Huntsville

ARIZONA
- Linda Kennedy, Unisource Energy Corp
- Charles Layton, L&L Health & Safety

ARKANSAS
- Zane Chrisman, USAble Life
- Bess Ginty, Kids for the Future, Inc

CALIFORNIA
- Sarah Agnetti, Amgen
- Cindy Anderson, Amgen
- Nicole Angell, Amgen
- Cathi Bowman, Amgen

- Molly Campos, Amgen
- Thomas Carague, Amgen
- Meegan Chute, Amgen
- Alana Cook, Amgen
- M. Jane Diaz, Ventura Foods, LLC
- Allan Diehr, National Semiconductor
- Nicole Erickson, Amgen
- Paula Evans, Amgen
- Noeleen Farrell, Community Health Clinic Ole
- Jessica Foster, Amgen
- Jason Garcia, Stanford University
- Katie Gibbs, Amgen
- Lauraine Guarino, Amgen
- James Guhl, Wal-Mart Stores
- Kathleen Hirose, Amgen
- Matthew Hudock, Amgen
- David Hudson, Aerojet General Corp
- Jeff Hunter, Amgen
- David Ab Jenkins, Cubic Corporation
- Deborah Jostes, Ethisphere
- Phoebe Kleiger, Amgen
- Anne Klezek, Amgen
- John Kunkel, Amgen
- Robert Le, Amgen
- Cathy Palmer, Amgen
- Avani Patel, Amgen
- Lisa Paulo, Salinas Valley Memorial Hospital
- Frank Pokrop, CareFusion Inc
- Katya Rivas, University of California Office of the President
- Lori Silver, Amgen, Inc.
- Sarah Soifer, Amgen
- Rosanne Stanford, Amgen
- Michael Stitcher, Aerojet
- Shannon Sullivan, Amgen
- Todd Tilk, Toyota Motor Sales USA Inc.
- Tanya Towns, Amgen
- Brian Warshawsky, University of California Office of the President
- Christopher Wingert, Amgen
- Rayna Wong, Amgen

COLORADO

- Karl Lueck, TIAA-CREF
- Kathleen Morgan, Crocs, Inc.
- Karine Wegrzynowicz, Crocs, Inc.

CONNECTICUT

- Maura E. Santos, Save the Children Federation Inc

FLORIDA

- Ronald Bazil, Children's Services Council of Palm Beach County
- Leyda L. Benitez, Florida International University
- Joann Campbell, University of North Florida
- Antonio Caram, Johnson & Johnson
- Beatrice Crapp, CMDI Solutions
- Joan Lee, IGPS
- Alicia Peters, Humana
- Caroline Preston, Johnson & Johnson
- Tonya Teschendorf, Wellcare Health Plans

GEORGIA

- Cindy Knezevich, The Network
- Deborah Newsholme
- Kirsten Schlau, The Network
- Sara Kay Wheeler, King & Spalding

ILLINOIS

- Karyn Boston, YMCA of the USA
- Dale Bridge, Navistar, Inc
- Jennifer DeMay, TCS Education System
- Tom R. Kiley, Great Lakes Advisors, Inc.
- John P. Killacky, Affirmative Insurance Holdings
- Amy Klaviter, Integrys Energy Services, Inc.
- Heather Ludlum, Great Lakes Advisors, Inc.
- Kevin Maffett, State Farm Insurance
- Steven Pearlman, Seyfarth Shaw LLP
- Kevin J. Rappel, Benedictine University
- Suj Shah, Ethically Managed/ MYECCHO
- Pamela Stewart, Allstate Insurance Company
- Nikita Williams, TCS Education System
- Justin M. Wozniski, Allstate Insurance Company

INDIANA

- Noreta Davis, NiSource
- Janice Teal, Advantage Health Solutions, Inc.

IOWA

- Laurie Buckhahn, Clarinda Regional Health Ctr
- Mayuri N. Farlinger, Alliant Energy
- Denise Hotopp, Visiting Nurse Services of Iowa

KANSAS

- Scott Wheatley, Lakemary Center

LOUISIANA

- Kirsten David, The Shaw Group Inc

MAINE

- Peter Falkson, National Sleep Therapy

MARYLAND

- Lynn Bartolotta, DoD
- Mike Gilberg, Allegis Group
- Ann Meeker-O'Connell
- Gregory Ray, Allegis Group, Inc.

MASSACHUSETTS

- Richard J. Daugusta, Dept of VA
- Paul T. Hempel, Alere Inc

MICHIGAN

- Earl C. Duby, Affinia Group Inc
- Jodie L. Earle, Holcim Inc
- Ingrid Flemming, Northern Michigan Regional Health System
- Ann V. Houston, Dorsey Schools
- Tammie McBain, Meijer
- Amy R. Popelar, Affinia Group Inc
- Tara Ragauss, CMS Energy

MINNESOTA

- Sherrie Schiebe, Zimmer Spine
- Jody Standal, Merrill Corporation

MISSOURI

- Janelle A. Martens, HNTB Corporation
- Edina Robinson, KCP&L

- Neal Schroeder, Enterprise Holdings Inc

NEBRASKA

- Diana Liska, First National Bank of Nebraska

NEW HAMPSHIRE

- William J. Dauksewicz, Liberty Mutual

NEW JERSEY

- Mike Ace, ImClone Systems
- Liz Allison, Johnson & Johnson
- Terry Camp, York Risk Services Group, Inc.
- Natalie Coniglio, McKesson
- Robert Criscuolo, VHA/CBI
- Scott Fabiano, ImClone Systems
- Jan Festa, Johnson & Johnsom
- Melissa Grandal, IEEE
- Karen Dougherty Green, Johnson & Johnson PRD, LLC.
- Aimee Hawkins, Johnson & Johnsom
- Eunice Jordan, JPMorgan Chase
- Robyn J. Labombarda, Dept of Veterans Affairs
- Hattie McKelvey, Johnson & Johnson
- Stephanie M. Pederson, Department of Veterans Affairs
- Richard H. Reed, ImClone Systems
- Christine Saus, Johnson & Johnson
- Elizabeth Schwartz, Johnson & Johnson
- Carmelo Stanco, Prudential Financial
- Spring C. Strickland, Dept of Veterans Affairs
- Kelly Talley, Johnson & Johnson
- Erika Varriale, ImClone Systems
- Naimish Vyas, Johnson & Johnson

NEW MEXICO

- Debra Gonzales, Optum Health

NEW YORK

- Christopher Barto, LIM College
- Luciana Bittar, New York Life International
- Francisca O.N. Brodrick, BONF International Enterprises
- Jay Cohen, Assurant Inc.
- Milagros Guzman, MF Global
- Charles L. Kyte, KRA-CRO
- Sean McPoland
- Nobuhiro Sawai, Sojitz Corporation of America
- John Zink, Rochester Institute of Technology

NORTH CAROLINA

- Roxane J. Stedeford, Talecris Biotherapeutics, Inc.

OHIO

- Annette Clavarella, Annette Clavarella Attorney At Law
- Mark A. Stach, Ashland Inc
- Mechelle Warner, Johnson & Johnson

OKLAHOMA

- Neal Lehman, ONEOK

OREGON

- Dana Kiel, Portland General Electric

PENNSYLVANIA

- Andrew B. Finkelstein, Coventry Health Care Inc
- Laurie Klann, Dick's Sporting Goods, Inc
- Samantha L. O'Donoghue, Dick's Sporting Goods, Inc
- Michele Rubincam, Johnson & Johnson
- Cathy Woodall, McKesson

PUERTO RICO

- Vladimir Roman Rosario, Inter American University of Puerto Rico

SOUTH CAROLINA

- Nichelle Cunningham, Force Protection
- Caryl J. Kuchman, SCANA Inc

TENNESSEE

- Jane B. Burns, University of Tennessee
- Eugene Fay, Capella Healthcare

TEXAS

- Shannon Dean, Pizza Inn Inc
- Vinita Kapoor, GenOn
- Gloria Martinez, Gila, LLC
- Joshua S. Roseman, Jones Day
- Dan Ross, Rackspace
- Joan Smith, GenOn Energy, Inc.
- Sheryl Starkey, Trinity Industries, Inc.
- Victor Vital, Greenberg Traurig, LLP

VIRGINIA

- Kiersten L. Boyce, The College of William and Mary
- Adelle Elia, GTSI Corp.
- Lizanne Kelley, Congressional Research Service
- Yousr Khalil, Baker Tilly
- Silva Miner, VeriSign
- Kim Neal
- Alice Faye Wells, Cape Fox Shared Services
- Walter Arnold, Altria
- Laurie Blackburn
- David Bourne, Deloitte
- Christiana Franchet, L-3 Communications
- Kristen Galloway, BRTRC
- Timothy Janes, Capital One
- Gregory Nixon, DynCorp International
- Charity Pomeroy, Ethos LLC

WASHINGTON

- Matthew Donohoe, Providence
- Dawn Mann, Microsoft
- David McMasters, Angiotech
- Shawna Stanley, Microsoft

WASHINGTON, DC

- Anne O'Connor, Chemonics International

WISCONSIN

- Donna J. Braatz, Alliant Energy
- Amy Coughlin, Assurant Inc.
- Julia M. Hix, Assurant Health
- David Tulbert, Assurant Inc.

The compliance and ethics initiative: Leading where skeptics don't even try

By Joe Murphy, CCEP

JOE MURPHY

Most of us in the compliance and ethics field have had our challenges: convincing managers, dealing with suspicious government officials, investigating difficult issues. But for the most part, we work in environments where the government is an actual enforcement threat, companies are large enough to retain us, and our clients actually exist on the record. But what would you do in a place where there was not a viable prospect of enforcement, companies were typically smaller than the smallest unit in most of our client companies, and the companies had not formalized their existence on the record? Welcome to the compliance and ethics initiative in Paraguay—where one local organization has organized more than 130 such companies to buy into compliance and ethics in a strikingly serious way.

Paraguay is a country that is ranked by Transparency International as being near the bottom in its corruption index, on a par with Ivory Coast, Yemen, and Papua New Guinea. This landlocked country, bordered by Argentina, Bolivia, and Brazil, has an agricultural economy and a population of six and a half million.

In this environment, Graciela Garay, Vice president of the American-Paraguayan Chamber of Commerce, has helped lead an initiative to bring business ethics and compliance to the businesses there. Working in the capital, Asuncion, the Paraguayan-American Chamber of Commerce and the Advertiser's Chamber of Paraguay have brought together the community to form an organization called Pacto Etico Comercial (PEC). At their initial meeting in 2004 to determine interest in the topic, she brought together more than 400 businesspeople. Today, the organization has more than 130 business members. Members run the organization and take ownership for its progress.

Among PEC's first initiatives was to bring the members over from the informal economy into a formal arrangement. Companies that had not given thought to incorporation, labor, and tax laws agreed to upgrade their approaches and become part of the formal structure. They agreed to adhere to labor regulations to ensure fair treatment of their employees, and they have moved toward compliance with other standards and the adoption of codes of ethics.

Thus far, the story would be impressive, but skeptics would note that such steps can still be "form over substance." After all, creating a code and living by one are two entirely different matters. Major multinationals that had elegant codes nevertheless engaged in outrageously illegal conduct; why would this be any different for small businesses in Paraguay? But this is where the story becomes most remarkable.

Members of PEC must have all their employees trained on the code, on business ethics, and on other requirements. But this is not something where PEC members can simply check off a box saying they have done this step. Instead,

CONTINUED ON PAGE 58

 CONTINUED FROM PAGE 57

PEC actually provides the training and will only sign off once a company's employees have actually been trained. Nor may the codes be created simply by downloading another company's code from the Internet and adopting it. Rather, the proposed company code must be circulated to all employees in draft, and their input and comments must be taken into account in the process. Members must train their employees on the code and have a system for employees to report concerns anonymously and without retaliation. There must also be a system for investigating and resolving such concerns.

How did Graciela get to this point? A Paraguayan native, Graciela also lived in the United States and worked for an American company, American Airlines. She attributes her experience at that company as the basis for her development of management skills. She received training on ethics and compliance through an initiative of the US Department of Commerce. Today she shares her story with leaders in other countries looking to improve their economies and ethical climates.

What motivates PEC members to participate? PEC will provide a certification to members who complete the requirements; a few have qualified thus far and more are scheduled this year. But, unlike some forms of external recognition programs that attempt to judge companies from afar, PEC requires actual in-depth checking. In this process, three of the Big Four accounting firms have signed on to conduct reviews at a discounted rate. But how do they know what to check? Is this just a financial accounting exercise? In fact, Graciela is the one who actually trains the accounting firms' personnel on how and what to check. This is a very impressive level of checking and assessment, but there is more. Graciela herself conducts on-site reviews of every certification candidate. And these are not merely check-the-box reviews; they include actual interviews of members' employees.

One concern about any certification is from the Law of Unintended Consequences. Once a program is certified, will the company then conclude it is finished and immediately shift attention to other matters? Will those working on the program move on to other matters, and will the program begin to fade away? Graciela is aware of this risk, and thus the certification is ongoing, and multileveled. No company is ever "finished"—there are more steps to pursue and ongoing assessments; companies must have periodic internal meetings as part of their programs.

What more do members have to do? Quite remarkably, they have learned the same lesson larger companies have learned: There absolutely must be someone in charge of the compliance and ethics effort in each company or otherwise nothing may happen. Each member, therefore, must designate a manager as responsible for the program, i.e., what we would consider a compliance officer. PEC members must perform checks on what they are doing, and hold employees accountable for following the rules. In other words, this is not simply an optimistic exercise in appealing to people's better natures and having everyone promise to be good. Rather, in Paraguay they are adopting approaches very similar to the lessons of the US Sentencing Guidelines and the OECD Good Practice Guidance.

What would the future hold for this initiative? The effort can extend to other parts of Paraguay outside of the capital. There is much more to do among the member companies to improve their efforts and their programs. For those with certification, there is the prospect of increased public recognition of their commitment to acting ethically and legally. They have already received important recognition from the government: The national customs authority gives PEC members "green light" treatment—expedited approval as a reward for their commitment. (One of the best examples of the type of incentive system to promote compliance programs that the OECD Working Group on Bribery's 2009 Recommendations call on members to do—done first by a non-OECD member country!)

More can be done in the future so that consumers in Paraguay understand the level of commitment by these companies. Equally promising is the potential for recognition by multinationals looking to do business in Paraguay. What better way for a company considering doing business in Paraguay to avoid risks of foreign bribery laws and demonstrate due diligence than to retain as a local representative a company that has its own compliance program, code of ethics, and compliance officer, with a built-in due diligence review?

Finally, for such a promising model, why stop at Paraguay? The need there certainly is great, but there are many others who might learn from Graciela and her colleagues. Her experience is a reminder that everywhere there are organizations, there is a need for the concepts of compliance and ethics; it may just take courage and persistence to bring about the change that is needed.

Here is the standard pledge given at each PEC meeting:

"We who gathered here, are ethical women and men, motivated by profound convictions and full of courage; people who carefully have determined and developed our own visions and are willing to accept that life is based upon proven values.

It is in our own and our generation's best interest to be successful with our commitment; and only if first we are willing to transform ourselves, will we be able to build an honest society based on ethical principles, so that it may become a more profitable and prosperous one."

Joe Murphy is of counsel to Compliance Systems Legal Group in Haddonfield, New Jersey and co-founder of Integrity Interactive Corporation (now part of SAI Global). Joe has more than thirty years experience and has worked on compliance and ethics matters on six continents. He is Co-Editor of *ethikos*, and has written several books and countless articles. He is a member of the SCCE board, and is SCCE's Director of Public Policy. Joe is also an avid ballroom dancer, and founder of the Society of Dancing Compliance and Ethics Professionals. Joe may be contacted by e-mail at jemurphy@voicenet.com or by telephone at 856-429-5355.

COMPLIANCE & ETHICS INSTITUTE *PREVIEW*

SESSION 705 **Are you Ready for the Global Competition Cops?**

Tuesday, September 13, 2:45–3:45 pm

BRADY DUGAN, Esq., Partner, Akin Gump Strauss Hauer & Feld LLP, Washington, DC

CHRISTINA HUMMER, LL.M, Partner, Saxinger Chalupsky & Partners, Brussels, Belgium

From industries as diverse as air travel to auto parts manufacturing, the governments in the U.S. and Europe are becoming increasingly aggressive in cracking down on cartel conduct. Techniques used by government agencies to uncover cartel conduct will be discussed. We will also consider how a company can qualify for amnesty in the different jurisdictions. Finally, we will suggest best practices for surviving a cartel investigation that is ongoing simultaneously in multiple jurisdictions.

SESSION 806 **Competing with Dodd-Frank: How to Keep your Hotline Alive**

Tuesday, September 13, 4:00–5:00 PM

STEVE EPSTEIN, Chief Counsel, Ethics and Compliance, The Boeing Company, Arlington, VA

The SEC is offering big $$$$ to your employees for allegations of corporate misconduct. How do you incentivize them to report internally first? Get the answers here. We demonstrate techniques to maximize employee use of your hotline and internal organizations to report their concerns. A little theory, but lots of practical advice. A great way to end the SCCE conference.

SESSION W1 **Workshop: Conducting Internal Investigations**

Wednesday, September 14, 9:00 AM–12:00 PM

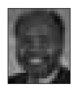
AL GAGNE, CCEP, Director, Ethics & Compliance, Textron Systems Corporation, Wilmington, MA

LATOUR "LT" LAFFERTY, JD, CHC, CCEP, Shareholder, Fowler White Boggs P.A., Tampa, FL

Conducting Internal Investigations Workshop: This workshop covers in a nutshell the basics for conducting effective internal investigations. Through the use of various scenarios workshop participants will focus on the importance for good intake from reporters, to planning the who, what, where, and how of the investigation process; to writing the final report and closing the loop with key stakeholders.

SESSION W2 **Building and Sustaining an Ethical Culture**

Wednesday, September 14, 9:00 AM–12:00 PM



RON JAMES, President and CEO, Center for Ethical Business Cultures, Minneapolis, MN

First Sarbanes-Oxley tried to do it! And now we are trying to do it with Dodd-Frank! No matter how hard you try, you can't legislate ethics and integrity! Yes we need to have rules and regulations that create a bright line between right and wrong! But the real challenge lies in navigating the "grey" areas.

Don't come to this session if you are looking for a "one solution fits all" answer. Rather, this session focuses on creating a framework for navigating in the grey areas of ethics and integrity. Join us to explore how great organizations are building and sustaining ethical cultures!

Attend SCCE's 10th Annual Compliance & Ethics Institute in Las Vegas, NV, to hear more!

Visit complianceethicsinstitute.org for complete conference and registration information.

Effective Internal Investigations *for* Compliance Professionals

A TWO-DAY WORKSHOP

NOVEMBER 10–11, 2011 | SAN FRANCISCO, CALIFORNIA

How Investigations Fit into the Context of Compliance Programs

Latour 'LT' Lafferty, CCEP, CHC, Practice Leader, Fowler White Boggs P.A.

Setting Policies and Guidelines for Conducting Internal Investigations

Al Gagne, CCEP, Director, Ethics & Compliance, Textron Systems Corporation

How to Plan an Investigation

Meric Bloch, CCEP, CFE, PCI, JD, Vice President-Compliance and Corporate Investigations, Adecco Group North America

Conducting Effective Interviews

Michael Johnson, Esq., Co-President, Global Compliance, Brightline Learning Division

Al Gagne, CCEP, Director, Ethics & Compliance, Textron Systems Corporation

Gathering Documentary Evidence

Meric Bloch, CCEP, CFE, PCI, JD, Vice President-Compliance and Corporate Investigations, Adecco Group North America

Forensics and Electronic Documents

Andy Teichholz, Daylight Forensic & Advisory LLC

Investigation Pitfalls and How to Avoid Them

Latour 'LT' Lafferty, CCEP, CHC, Practice Leader, Fowler White Boggs P.A.

Preparing the Report

Al Gagne, CCEP, Director, Ethics & Compliance, Textron Systems Corporation

Meric Bloch, CCEP, CFE, PCI, JD, Vice President-Compliance and Corporate Investigations, Adecco Group North America

Discipline, Follow Up and Closing the Loop

Al Gagne, CCEP, Director, Ethics & Compliance, Textron Systems Corporation

Investigations Roundtable

Al Gagne, CCEP, Director, Ethics & Compliance, Textron Systems Corporation

Michael Johnson, Esq., Co-President, Global Compliance, Brightline Learning Division

Meric Bloch, CCEP, CFE, PCI, JD, Vice President-Compliance and Corporate Investigations, Adecco Group North America

Latour 'LT' Lafferty, CCEP, CHC, Practice Leader, Fowler White Boggs P.A.

To learn more and register, visit
www.internalinvestigations.org

SCCE
Society of Corporate Compliance and Ethics