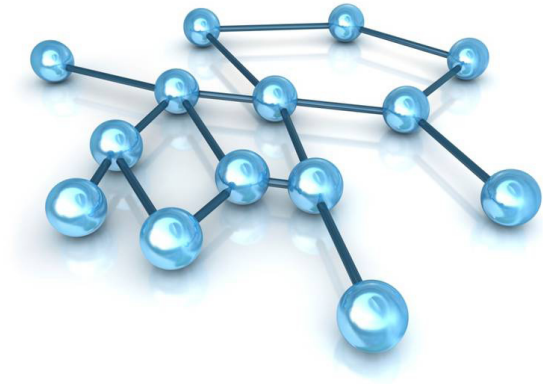


Applying six degrees of separation to preventing fraud



by Yogesh Bahl

Companies are increasingly exploring ways to take tools and techniques used in fraud investigations and apply them proactively to help prevent and detect corporate fraud before it does serious damage. One such opportunity involves considering the human element of corporate fraud and leveraging the work of the company's specialists, including those in the Human Resources (HR) function.

This approach can be especially valuable when your business is global and you are managing risk among subsidiaries in various countries around the world. In addition, given strong government enforcement of potential violations of the Foreign Corrupt Practices Act (FCPA), understanding relationships among company representatives and foreign government officials can be invaluable for helping to avoid prohibited transactions.

Theories of human interaction and behavior: Six Degrees and Group Polarization

It can be beneficial to consider two theories involving human interaction and behavior. One, the theory of Six Degrees of Separation, which asserts that every person on Earth is connected to every other person by no more than six steps; and two, the concept of Group Polarization, which refers to the tendency of people in groups to be swayed to one extreme or the other through their interaction within the group¹.

According to the 2007 *National Business Ethics Survey* of nearly 2,000 business-people, conducted by the nonprofit Ethics Resource Center:

- 56 percent of respondents had personally observed conduct that violated company ethics standards, policy, or the law in the past twelve months.
- 42 percent of respondents who observed misconduct chose not to report it.
- Non-reporting of bribes was 64 percent.
- The most commonly observed form of misconduct was people putting their own interests ahead of those of the organization (22 percent).

How are these theories relevant to fraud and the mitigation of fraud risks? According to the "Fraud Triangle," originally developed by criminologist Dr. Donald Cressey, the following elements are usually present for fraud to occur:

- **Perceived opportunity to commit the fraud with low likelihood of detection** — for example, if controls are missing or inadequate, or the perpetrators have the ability to override controls. Six Degrees of Separation applies here as the opportunity to commit fraud may become greater when more individuals are connected directly or indirectly, enabling collusion to take place.
- **Pressures/Incentives** — for example, the perpetrator will gain financially from the fraud or feels pressured to "make his numbers." This is where Group Polarization may come into play, when individuals who are essentially honest are swayed by others who take extreme views. So, for example, a CFO tells

¹ Sunstein, Cass R., *The Law of Group Polarization* (December 1999). University of Chicago Law School, John M. Olin Law & Economics Working Paper No. 91.

the head of accounting that his view of revenue recognition is wrong and convinces him to take another course of action he initially would not have chosen, thereby allowing for management override of controls.

- **Rationalization** — for example, “The company won’t miss this money” or “We need to show a profit this quarter.” An individual’s personal views of entitlement and ability to execute with impunity can influence the individual’s actions.

Connections can be key

Microsoft researchers gave the premise of Six Degrees of Separation a modern twist, studying the instant-messaging habits of users on the Microsoft Messenger network. After examining the 30 billion messages sent during June 2006, researchers concluded that it would take an average of 6.6 steps to connect all the users in the database and that 78 percent of the pairs could be connected in seven links or fewer².

Whether or not you buy into the Six Degrees of Separation premise, it suggests the possibility for companies to help mitigate their fraud risks by seeking out undisclosed connections among individuals. Fraud risk factors can take on a different life when more people are associated via common or complementary interests, goals, and objectives. In investigating allegations of fraud, a number of electronic tools can be used to help identify these relationships, especially those that are not obvious.

People involved in corporate fraud generally have similar or complementary incentives and pressures and, ironically, need to trust

one another in order to capitalize on the trust of others. Trust typically requires longer-term relationships or association. Often businesspeople who commit fraud might be connected beyond the fraudulent act: They may belong to the same country club, their spouses may share common interests, or their children may go to the same school. A relationship outside of work can establish trust, and the rationalization and collusive elements of fraud may be based on years of relationship building — years before any fraud occurs.

In addition, common incentives/pressures and trust can be further reinforced within the work environment, potentially heightening the risk of fraud. Awards for meeting sales goals, bonuses linked to share price, and similar practices can mix the corporate realm of policy with the personal realm of everyday interaction and relationships. More specifically, two people who have a personal relationship may also have a stake in meeting related goals, whether they work in the same company or in companies that do business together.

Moreover, take the example of a potential FCPA violation, where someone in your sales force or an agent is selling to a hospital owned by a foreign government. Understanding the relationships among the involved individuals before the sales transaction can be valuable to understanding the risk exposure. Similar examples can relate to money laundering and liability created by agents serving on your behalf, such as international expeditors in the construction industry.

² BBC News story, published 8/3/2008, <http://news.bbc.co.uk/1/hi/technology/7539329.stm>

Integrating the human factor in your fraud risk management program or due diligence efforts

Supplementing antifraud controls with activities to uncover undisclosed interpersonal connections can enhance your overall fraud risk management program without being overly burdensome. Also, keep in mind that these techniques can be used when you are performing due diligence in an M&A transaction or strategic alliance deal, particularly when the work spans country borders. You may consider the following measures:

1. Laying the groundwork up front for more effective background checks and integrity due diligence.

Relationship trees may be used in fraud investigations to show connections between people and corporations and to reveal how assets were moved, what journal entries were used, and the like. Taking a similar mapping approach to uncover personal connections early on, prior to conducting background checks on potential new hires or vetting potential vendors or other business partners, can make those later investigations more effective. This can be valuable, particularly when conducting global due diligence.

Strategic interviewing can reveal who knows whom, how they know each other, and where commonalities are, such as familial relationships and shared clubs, hobbies, or other interests. Questions can be focused on relationships beyond work-related ties and titles, including professional and fraternal organizations. Because these connections can be forged at any time, regular checks of key decision makers or influencers (say, the person in charge of

vendor relationships for the company and the person on the vendor's end responsible for day-to-day account management) can be beneficial.

If you do find such relationships, either initially or down the road, you can have a process in place to explore the nature of the relationship and determine whether it could bias future decision making. Ultimately, you may need to make a change that distances the parties or document why you think a relationship does not pose undue risk. It is important to involve relevant individuals in any decision, such as the chief compliance officer and in-house counsel.

2. Expanding typical interview questions to encompass personal connections.

When conducting interviews, whether as part of an internal audit process or in the course of an investigation, you may consider asking if there are connections beyond the day-to-day professional relationships. Please keep in mind that certain lines of questioning should be approved by counsel in advance.

3. Augmenting antifraud processes to include relationship evaluation.

Common antifraud processes may benefit from consideration of the impact of relationships (Six Degrees of Separation) and influence (Group Polarization). Such processes may include:

- Brainstorming potential fraud risks and schemes and mapping them against current controls to uncover gaps
- Conducting fraud diagnostics to compare current fraud management practices to leading practices or peer companies
- Monitoring transactions for potential fraudulent activity

For example, fraud schemes can be mapped against individuals who appear to share common relationships and incentives/pressures. This type of quantitative information can be combined with qualitative information from other, often untapped corporate sources.

4. Relating fraud risk management to people management.

Some people may not think of the HR function as a preventive control against financial fraud. In fact, HR can play a key role in fraud prevention and detection in the course of its routine activities. As previously mentioned, pre-hire background checks can examine “Six Degrees Relationships” as a fraud-mitigation tactic, and performance review results can be analyzed against potential fraud indicators. In addition, HR can confirm that proper termination processes are in place and are being followed, such as quickly denying terminated employees’ access to critical systems and informing key clients or vendors of the termination.

In particular, the HR function generally has the most extensive information about a company’s people and may be able to help identify people who appear to be under more pressure than normal or perhaps are doing unusually well, such as a sales representative generating much more revenue than his peers. HR can also be a valuable resource in understanding the impact of reward and incentive programs. The corporate security function may also be a source of information helpful in evaluating potential fraud risk — for example, has somebody been accessing systems or areas when they were not allowed? Has this person also raised red flags in HR?

5. Integrating relationship identification in your fraud response management process.

Many companies still do not have a formalized fraud response management process in place nor what we call a ‘Playbook,’ which can provide a step-by-step approach to handling fraud allegations. This can be the first step in managing the risk around allegations of fraud and the fraud itself. Such a Playbook can integrate relationship mapping techniques and HR involvement to potentially increase the effectiveness and efficiency of the investigation.

The bottom line: Considering and integrating human interaction and socializing behaviors can help mitigate fraud and other compliance risks

Beyond the obvious financial loss, fraud can take its toll in reputational damage, in diverting focus from core business activities, and in investigatory costs and resource requirements. Compliance with regulations and fraud risk mitigation programs can also be costly, though necessary, endeavors. Considering the human element of fraud and channeling information and specialized resources already in your company toward that effort could help you reduce your risks.

This article and corresponding DVD were first published as part of ForThoughts, the Deloitte Forensic Center's newsletter highlighting the trends and issues in fraud, corruption, and other complex Business issues. To subscribe to ForThoughts, visit www.deloitte.com/forensiccenter or send an e-mail to dfc@deloitte.com

Yogesh Bahl is a partner and the Northeast Leader of Anti-fraud Consulting for Deloitte Financial Advisory Services LLP. Yogesh specializes in helping companies develop customized and more effective solutions to prevent and respond to allegations of fraud. In addition, Yogesh has conducted global investigations involving various allegations of improper business practices.

The views expressed in this publication are solely those of the author and not necessarily those of Deloitte Financial Advisory Services LLP.

This publication contains general information only and Deloitte Financial Advisory Services LLP is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte Financial Advisory Services LLP, its affiliates and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

Deloitte Forensic Center

The Deloitte Forensic Center is a think tank aimed at exploring new approaches for mitigating the costs, risks and effects of fraud, corruption, and other issues facing the global business community.

The Center aims to advance the state of thinking in areas such as fraud and corruption by exploring issues from the perspective of forensic accountants, corporate leaders, and other professionals involved in forensic matters.

The Deloitte Forensic Center is sponsored by Deloitte Financial Advisory Services LLP. For more information, visit www.deloitte.com/forensiccenter.

About Deloitte

As used in this document, "Deloitte" means Deloitte Financial Advisory Services LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.