J.H. COHN LLP
ACCOUNTANTS & CONSULTANTS

LECLAIRRYAN

Hedging Your Bets Against the Whistleblower Trifecta

Protection and Prevention in the Era of the Dodd-Frank Act, Foreign Corrupt Practices Act, and False Claims Act

Whistleblower Rules and Incentives Spur Additional Fraud Reports and Require Companies to Prepare, Respond

The passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") and the 2010 debut of the Security and Exchange Commission's ("SEC") Office of the Whistleblower have greatly increased the incentive for a whistleblower to come forth with information about corporate wrong-doings. Today, in light of potential rewards and proffered protection, the motivation to report fraud to the Department of Justice ("DOJ") or the SEC is greatly increased. As a result, companies must evaluate their anti-fraud and anti-bribery/corruption policies and processes to further insulate themselves against events that could lead to a DOJ/SEC investigation and significant fines and costs.

Recently, executives from LeClairRyan, an entrepreneurial law firm, and J.H. Cohn LLP, one of the leading audit, tax, and consulting firms in the United States, gathered at the Union League Club in Manhattan to discuss the impact of increased regulation, the renewed focus on regulations surrounding bribery and corruption, and the resulting increase in claims, and what companies can do to prevent as well as handle allegations of fraud, bribery, or other corporate wrongdoings. The following is a summary of the issues discussed.

Whistleblower actions are nothing new, but with the advent of new regulations and increased enforcement by the DOJ and SEC pertaining to the Foreign Corrupt Practices Act of 1977 ("FCPA"), along with similar regulations in many foreign countries, whistleblower motivation, claims, and awards have risen substantially. In fact, in just the first few weeks of the SEC's whistleblower program almost 400 tips were received by the SEC. Clearly, as these claims are just starting to go through the Office of the Whistleblower, 2012 will likely be known as "the year of the whistleblower."

In fact, rewards now have the potential to range between 10 percent and 30 percent of monetary sanctions collected as a result of regulatory action, and an "open-door policy" means that all with cause are welcome to blow the whistle on perceived wrongdoing, anonymously, with the added bonus of protection against retaliation. Awards to whistleblowers in the millions of dollars are becoming much more prevalent. A "bounty hunter" mentality is setting in and companies must aggressively assess their internal policies and compliance programs to have any chance of successfully navigating these potentially troubled waters.

The Role of the Foreign Corrupt Practices Act in Detracting Criminal Activity

Triggers for whistleblower actions may include securities fraud, healthcare/Medicare fraud, or significant internal control deficiencies but consensus is that the FCPA has been a major driver for reform.

The FCPA, which is jointly enforced by the SEC and the DOJ, prohibits U.S. companies and citizens, foreign companies listed on a U.S. stock exchange, or any person acting while in the U.S. from corruptly paying or offering to pay, directly or indirectly, money or anything of value to a foreign official to obtain or retain business (commonly referred to as the Antibribery Provisions). The FCPA also requires issuers with securities traded on a U.S. exchange to (1) file periodic reports with the SEC, (2) keep books and records that accurately reflect business transactions, and (3) maintain effective internal controls. This rule was made to help ensure that transactions are executed according to management's general or specific authorization and that they are recorded to permit the preparation of financial statements in conformity with generally accepted accounting principles, and to maintain accountability for assets.

The repercussions for noncompliance are harsh and may include such disciplinary action as fines, prison, civil penalties, and debarment from contracting with the U.S. government. And it's not the alleged wrongdoers who would be responsible for the accused actions, said William A. Despo, a LeClairRyan shareholder and leader of the Firm's Financial Services Litigation and Regulation team.

"It is possible for a parent company to be held responsible for the conduct of its subsidiaries under SEC rules even if it had

no knowledge or suspicion of FCPA violations," said Despo. Today, greater resources are being dedicated to FCPA compliance than ever before. The DOJ has reported that it prosecuted more FCPA cases in 2008 and 2009 than in the preceding 20 years combined. Improved information-sharing arrangements and prosecution by foreign regulators, both via treaties and informal arrangements, have gone far in cracking down on FCPA violations, as have industry-wide probes, the prosecution of individuals, and the potential for reward. Further, stiffer corporate and civil penalties and a more stringent focus on non-traditional bribes and payments made through intermediaries, such as agents or consultants, have detracted from any remaining allure that an FCPA violation may hold, regardless of perceived short-term gains.

"It now goes beyond cash exchanges," said Anthony Zecca, CPA, managing partner of Cohn Consulting Group, a division of J.H. Cohn LLP. "Now, the DOJ and SEC are looking at travel and entertainment, charitable donations, family perks—essentially anything of value—and there is no materiality factor."

Carlos Ortiz, a shareholder at LeClairRyan added, "The new provisions are a game changer. There is so much money on the table, it is too much to ignore. There is now a global army of lawyers and forensic accountants working for the DOJ and SEC who are actively investigating allegations, pursuing higher fines, and sharing information across borders, making it almost impossible for perpetrators to escape."

The FCPA compliance program, for its strengths, continues to evolve and is subject to its own potential downsides. Though considered a "gold standard" compliance program on paper, deficiencies exist in numerous areas, including the dedication of resources to ensuring the control objects are being met and resources charged with ensuring the program is implemented and fully functioning throughout the company. Further, third-party risk mitigation and education remains an ongoing problem, as do varying interpretations of FCPA by international bodies. The UK Bribery Act, for example, has a much broader definition than does the FCPA, which in turn requires additional compliance research to be conducted by an entity prior to engagement in foreign activities.

"In certain countries, corporate officers say that bribery is a natural course of getting business done but leadership has to enforce an international anti-fraud corporate culture," said Cohn Consulting Group's Zecca. "Management needs to take a stand and simply not do business in countries where that is the modus operandi, because that is no longer a excuse or defense against violations of the FCPA." In many ways, he added, the only good defense is a very strong, documented, and carefully executed compliance program, which demonstrates that a company took reasonable steps to prevent the FCPA violation.

> "Boards need to ask, what is our plan, what do we need to do, what are our procedures. A code of conduct must be put in place, and whistleblower procedures must be formalized. Good employee communication is key, as is being a good corporate citizen."
>
> *Anthony Zecca, CPA, Cohn Consulting Group, a division of J.H. Cohn LLP*

The False Claims Act: Protecting Government Programs from Fraudsters

The False Claims Act ("the Act") is of particular relevance to government programs, such as Medicare, that are susceptible to fraud. The Act imposes liability on persons and companies who defraud governmental programs. Revised whistleblower provisions under the Act eliminate the previous need for whistleblowers to be internal sources and allows for the sharing of knowledge that "materially adds" to any prior publicly disclosed claims and any knowledge that materially assists. First-hand knowledge is no longer required. The impact of these changes has been significant: in the two-decade period between 1987 and 2008, the government recovered nearly $22 billion in response to the whistleblower program.

The liability outlined under the Act leaves little room for discussion and is applicable whenever a person improperly

received payment from the Federal government or avoids making payment to the government. Though the Act's impact reaches a wide swath of industries and markets, it has a particularly noticeable effect on the nation's Medicare system. As such, the act of knowingly presenting, or causing to be presented, a false claim for payment or approval or knowingly making, using, or causing to be made or used a false record or statement material to a false or fraudulent claim, is exposed to the rules.

Fraud and the Role of Ethics in Its Existence

Fraud, including bribery, occurs for three primary reasons, frequently referred to as the "fraud triangle": opportunity, rationalization, and pressure or incentive. For any type of fraud to occur, would-be criminals are able to identify gaps within existing controls and determine how they may be over-ridden; rationalize the activity on the premise that they are "owed" by the company or that it is for the greater good; and succumb to the allure of financial or reputational gain. The means to perpetrating the crime are just as varied and may include financial misstatement, business practice fraud, the misappropriation of assets, and corruption or bribery.

However, for the rational categorization it is critical to remember that fraud, more than anything else, is an ethical issue.

"People will behave in a way that is condoned by senior management, in a way that reflects their perception of the organization," said Zecca, suggesting that there is a direct correlation between an organization's tone at the top and its ethical culture.

An organization's ethical culture is driven by policies and procedures, training processes, and a clear communications channel—items perpetrated across the top by senior management, operating management, and the audit committee. But the failure of secure controls at the management level, Zecca suggests, is often the impetus for employee fraud. They're very different, however. While management fraud tends to be "relationship-driven" and oriented toward bribery, corruption, and collusion, employee fraud tends to almost always be "against the organization" and primarily comprised of asset misappropriation.

"Management fraud occurs five times as frequently as employee fraud, and is most frequently perpetrated by a high-profile, senior-level executive," he added. "Employees interpret what they see, not what they hear, which speaks to the absolute need for controls."

Understanding Fraud

Fraud can be committed in a variety of ways: abuses of trust committed by people in organizations for personal profit; business crimes committed by organizations to further their business interests, e.g. false earnings reports; or confidence games designed to cheat clients, e.g. Bernie Madoff's Ponzi scheme. According to J.H. Cohn's Anthony Zecca, there are four key questions to examine:

- **Why does fraud occur?** It can be boiled down to the fear and greed of companies and individuals. Companies have earnings pressures brought on by stockholders, venture capitalists, and impatient financial analysts. Individual greed can also lead to fraud. Executives whose compensation and bonuses are tied to revenues are prime candidates to commit fraud.
- **How does fraud occur?** A company with strong leadership will make sure that proper controls are in place to prevent fraud. Companies that have poor internal controls, no ethics policies, or policies in place which allow management to override controls are prime candidates to be victimized by fraud.
- **How does fraud manifest itself within a business?** Companies can commit fraud in a variety of ways, including the acceleration of revenue recognition, expense capitalization, inventory manipulation, overstatement of receivables, disbursements to fictitious vendors, unsubstantiated valuations of assets, and intra- and inter-company activities.
- **How are frauds discovered?** From good internal controls to serendipitous accidents—and everything in-between. Employees, customers, suppliers, and auditors are all candidates for discovering fraud.

Fraud: An Ounce of Prevention

The detection of fraud generally occurs as a matter of course, not as a result of organizational policy or culture. Having a strong risk management program in place is essential, as is having a formal process for researching potential problems.

"First and foremost, you need a fraud risk management program in place that includes written policies of conduct," said Richard Salute, J.H. Cohn partner and director of the Firm's Capital Markets and SEC Practice. "You need to establish prevention techniques, including formal policies, procedures, training, and communication. And you need to solicit input, on the enterprise level, and coordinate your approach to risk management."

Zecca added, "Many companies fall victim to fraudulent activity because they believe that 'it can't happen here,' that programs like Sarbanes-Oxley protect them from fraud, or that any fraud that might take place would quickly be discovered. In fact, all companies are vulnerable to fraud and no individual fraud detection system is foolproof."

There is the case, argued Zecca, for an integrated approach to fraud prevention and detection, one that includes corporate governance (the culture, values, mission, structure, and layers of policies, processes, and measures by which organizations are directed and controlled), risk management (the systematic application of processes and structures that enable an organization to identify, evaluate, analyze, monitor, improve, or transfer risk while communicating risk and risk decisions to stakeholders), and corporate compliance (the ability to demonstrate adherence to mandated requirements defined by laws and regulations).

"An integrated approach to fraud prevention and detection takes into consideration financial risks, operational risks, and compliance risks," he said. "The success of any fraud prevention and detection system is contingent on the commitment and dedication that boards and senior management give it."

The detection of fraud should include such basic corporate policies as the conduct of surprise audits of high fraud risk areas; fraud awareness and focus on every audit; continuous monitoring; trends and analytics of financial and non-financial measures; and continually listening and watching for red flags. Salute further emphasized five policies that every board of directors and member of management should consider when it comes to risk:

> "Most people do what they think is right, considering the world they think they live in."
>
> *The Ethical Process, Marvin Brown (2002)*

1. Create a fraud risk management program and include written policies. This should include such items as fraud awareness, a periodic affirmation process, fraud risk assessment, reporting procedures and whistleblower protection, and a formalized investigation process.

2. Assess the company's fraud risk exposure. Assess existing incentives, pressures, and opportunities for fraud to occur and consider the implementation of management controls to enable process override should a fraud event arise.

3. Establish prevention techniques. Put policies and procedures in place and initiate training so employees and management are aware of each. Thorough communication is key for supporting a fraud prevention and reporting program.

4. Establish detection techniques. This includes detection controls to support a fraud prevention problem in the event that organizational weaknesses are uncovered.

5. Solicit input and create a coordinated approach to investigation and corrective action. Develop a system for prompt resolution of fraud allegations and establish a process to evaluate allegations.

When Fraud Occurs

If, despite preventative measures, fraud is suspected, there is a seven-step program to be followed, explained a panel comprised of Kevin Clancy, CPA, a J.H. Cohn partner, co-leader of the Firm's Business Investigation Services Group; Carlos Ortiz, Esq., shareholder, LeClairRyan; and Michael Ruggio, Esq., shareholder, LeClairRyan.

Step 1: Conduct an initial assessment. Identify the whistleblower. Is the complainant a current or former employee, or is it an outside party (e.g., a competitor or a distributor)? Next, examine the claims. Do they relate to violations of Federal or local law, industry regulation, or company policy?

Determine whether the complaint requires an investigation. U.S. Sentencing Guidelines require "reasonable steps" to respond appropriately to detected criminal conduct and the Office of Inspector General Model Guidance requires a company to "immediately investigate" issues to determine whether a material violation of law has occurred. Foreign regulatory offices take a similar approach.

Step 2: Interview the whistleblower. An early and comprehensive interview is critical. Keep in mind that this may be the only opportunity to interview the whistleblower, so the interview must be as thorough as possible and address evidence, parties that may be involved, and knowledge of the occurrences, as appropriate.

Step 3: Preserve and collect documents and evidence. Preserve the sanctity of existing data and documents by initiating a document hold. Suspend routine document retention and destruction procedures to preserve documents potentially relevant to the investigation. Work with IT to preserve hard drives, tapes, documents, and digital evidence in accordance with legal guidelines and rules of evidence. It's also important to find and collect electronic data, wherever it may be located, and analyze it to locate, identify, and extract information of evidentiary value to the investigation.

Consider alternative sources of documents, including those that may be in the control of a "key" witness, and be mindful of data privacy and protection laws that may prevent the extraction of such files from a potential witness's database.

"There are certain restrictions on whether you may process data and how you may process it. Also, it is critical that as each stage of processing is undertaken you have a basis in law, which generally includes appropriate consent and necessity," Clancy added. "There are really no exceptions, and where conflicts have existed, such as in the case of contraction between U.S. and EU law, a government-to-government negotiation is required."

Step 4: Conduct a financial analysis. Document the path of all funds involved in the alleged fraud and reconstruct the data. Review and analyze historical and current financial results, look at transactions among all parties involved, and thoroughly analyze all supporting documents related to the transactions in question, including contracts, invoices, checks, and wire transfers.

Step 5: Interview witnesses. Speak with all witnesses identified by the whistleblower. It is critical that counsel provide the same warnings and requests provided to the whistleblower, and present the evidence gathered and ask for an explanation or response.

Step 6: Analysis and conclusions. Review all documents and evidence gathered and determine the credibility of the claim, the witnesses, and the integrity of data collected. If the complainant's claims are corroborated, work with advisors to create a written report of the investigations done to date.

Step 7: Resolutions and action. Post-investigation, consider if any or all of the following are warranted or required: additional training, enhanced controls, consultation with HR

The Cost of Fraud to U.S. Businesses

Source: Association of Certified Fraud Examiners, Inc. (2008)

- More than 60 percent of the organizations surveyed had a fraud loss in excess of $100,000.
- Median loss was $178,000 with more than 25 percent greater than $1 million.
- A typical U.S. organization loses seven percent of its annual revenue to fraudulent activity. Applying seven percent to the estimated 2008 U.S. GDP of $14.2 trillion, that would equate to approximately $994 billion lost to fraud in 2008!

regarding appropriate disciplinary action, and a response to the complainant.

The resolution of an investigation also brings to light the potential need for disclosure and of notice obligations. Work with advisors to determine who needs to be notified internally (boards, audit committees, etc.), externally (i.e., SEC disclosures), as well as to other third parties (i.e., outside auditors, lenders, and business partners). Disclosure to the government is frequently a topic of heated debate, but in reality there are three potential outcomes, added LeClairRyan's Ruggio. They are:

1. No disclosure, and conduct does not come to the attention of regulators in the U.S. or abroad. While this eliminates the possibility of fines, monitoring, DOJ- and SEC-mandated investigations, it also carries with it the uncertainty of whether a discovery will happen within the next five years via a whistleblower, an industry probe, or an acquisition.

2. No disclosure, and conduct does come to the attention of regulators in the U.S. or abroad. Immediately, the organization is at a detriment as it is forced to justify why the information was not disclosed and there may be certain preconceptions of conduct that will need to be overcome. While it is possible to overcome these challenges, doing so is frequently difficult.

3. Full disclosure. While the organization will face a potential fine and be subject to potential additional investigation, organizational credibility with the DOJ and SEC is enhanced and the opportunity exists to frame the issues as opposed to responding to allegations. The government may also be inclined to reduce fines or dismiss an investigation all together.

"There are choices to be made, and each has its pros and cons based upon the organization, the action perpetrated, and the outcome," concluded LeClairRyan's Ortiz. "It's impossible to say which is best, but there is no question that the implementation of an effective fraud risk management program will best prepare any company for whichever scenario presents itself."

Contact Information

J.H. Cohn LLP

Anthony Zecca, CPA
Managing Partner, Cohn Consulting Group, a division of J.H. Cohn LLP
azecca@jhcohn.com
973-871-4020

Richard Salute, CPA
Partner and Capital Markets and SEC Practice Director
rsalute@jhcohn.com
516-336-5501

Kevin Clancy, CPA, JD, CIRA, CFF
Partner and Business Investigation Services Group Co-Leader
kclancy@jhcohn.com
732-635-3108

LeClairRyan

William A. Despo
Shareholder
William.Despo@leclairryan.com
973-491-3325

Carlos F. Ortiz
Shareholder
carlos.ortiz@leclairryan.com
973-491-3365

Michael F. Ruggio
Shareholder
michael.ruggio@leclairryan.com
202-659-6719

James P. Anelli
Shareholder
james.anelli@leclairryan.com
973-491-3550

J.H. Cohn LLP
4 Becker Farm Road
Roseland, NJ 07068

LeClairRyan
One Riverfront Plaza
1037 Raymond Boulevard
Sixteenth Floor
Newark, New Jersey 07102