

October 13, 2014

## Government's Message to Corporate America — "We Want Your Whistleblowers!"

By Earl "Chip" Jones III, Philip Storm, and Amy Mendenhall

On September 22, 2014, the Securities and Exchange Commission's (SEC) Office of the Whistleblower announced that it had issued a \$30 million bounty payment to a foreign whistleblower. This award is more than double the amount of any previous payment issued by the Office of the Whistleblower and comes fast on the heels of a \$300,000 payment to a whistleblower who worked as a compliance professional. The magnitude of the \$30 million award and the payout to a company's own compliance advisor underscore a fundamental shift in enforcement strategy among regulatory agencies—a shift from encouraging internal corporate compliance to policing corporate conduct by encouraging employees to report directly to the government.

Listen to any government regulatory chief within the past year, and you will hear a consistent refrain encouraging whistleblowers to report misconduct outside the company and promising protection from retaliation, significant penalties against organizations, and personal financial rewards that can reach into the many millions of dollars. The take-away for employers is simple: improve your internal whistleblower response systems and your ethics and compliance programs or face the consequences.

The creation of the Dodd-Frank Act bounty program first signaled this public policy shift. Prior to Dodd-Frank, organizations were encouraged to develop methods of self-regulation. For example, the Sarbanes-Oxley Act required organizations regulated by the SEC to adopt Codes of Ethics and implement anonymous, confidential compliance hotlines. While those requirements still exist, Dodd-Frank ushered in a new era in which the government uses the lure of potentially multi-million dollar bounty awards to transform even rank and file employees into enforcement agency informants. In other words, the message since the enactment of Dodd-Frank has become, at least in part, "we don't trust your ability to self-regulate, and we will entice your employees to turn you in."

With the increasing pace and amounts of bounty payments issued under Dodd-Frank, we are now beginning to experience the full force of this policy shift. Although the SEC's Office of the Whistleblower issued only a handful of awards during the first years of the program, these recent bounty payments suggest that employers should be anything but complacent.

Sean McKessy, Chief of the SEC's Office of the Whistleblower, says his staff is dedicated to rooting out impediments to external reporting and finding appropriate whistleblower retaliation claims to pursue. He has repeatedly said the best thing companies can do to avoid his office is create a culture where employees feel comfortable reporting matters internally and where management has a process in place that results in credible, transparent investigations. Other SEC officials have publicly stated that companies subject to investigation by the SEC would do well to showcase comprehensive, effective compliance programs and internal investigation capabilities. This advice from the SEC is familiar, echoing the 2012 Foreign Corrupt Practices Act Resources Guide jointly released by the SEC and DOJ in which the agencies emphasized that a well-designed and fairly enforced compliance program can help prevent violations, detect those that occur, and remedy them promptly.

For companies that do not have such compliance programs, the SEC's Office of the Whistleblower is prepared to light a fire. At a recent nationwide compliance conference with approximately 1,500 compliance officers and professionals in attendance, McKessy told the audience he was there "trolling for tips" and that the compliance professionals were all invited to bring those tips to the SEC.

McKessy also emphasized, not for the first time, that the SEC has the independent authority to prosecute retaliation claims and is actively working to identify and penalize organizations that take action to dissuade whistleblowers from reporting to the SEC. In addition to protecting individuals who report to the SEC, the SEC is looking for organizations that have created agreements, such as severance, confidentiality, and employment agreements, with terms intended to dissuade employees from reporting to the SEC. McKessy has threatened that attorneys who draft such documents might have their ability to practice before the SEC revoked by the agency.

The redoubling of enforcement efforts and efforts to cultivate whistleblowers is also occurring outside of the SEC. The Department of Justice's Chief of the Criminal Division, Leslie R. Caldwell, recently described that agency's increased focus on Medicare fraud, defense procurement fraud, and financial fraud/bribery. The DOJ plans to commit more resources to False Claims Act cases and will actively work cases cooperatively between the criminal and civil divisions. Further, Attorney General Eric Holder recently proposed dramatic increases in the amount of awards available to whistleblowers in the financial sector as part of an effort to increase individual cooperation and improve upon the effectiveness of DOJ investigations.

## Recommendations for Employers

To help construct a bulwark against these increased government enforcement efforts and efforts to entice would-be whistleblowers, including even an organization's compliance and audit professionals, employers should work with knowledgeable counsel to take the following critical measures:

1. Review and analyze the company's Ethics and Compliance Program. An outsider's objective and expert review of the ethics and compliance program can help identify gaps and areas for improvement. The Federal Sentencing Guidelines for Organizations also requires this kind of periodic assessment.
2. Update and elevate the importance of anti-retaliation policies and procedures and re-train employees and executives at every level. Many organizations still have a very weak policy generally prohibiting retaliation, and they do not train managers that potentially insignificant decisions can lead to an employee believing that he or she is the victim of retaliation. Fear of retaliation can prevent employees from coming forward internally with reports of misconduct and may increase the likelihood that they will take their concerns directly to the government.
3. Ensure that your organization has a comprehensive incident management system. Recent research shows that only 3–5 % of reports of misconduct are made through a helpline. Supervisors and managers receive the vast majority of such reports. If those supervisors and managers do not properly escalate those reports, the organization will never have the chance to remediate and rectify.
4. Develop investigation protocols and train. Conducting effective and lawful investigations is no longer a luxury for an organization; it is a necessity. A well-designed investigation system will better ensure that all important legal and compliance issues are identified, tracked, and resolved.

5. Review and update your organization's Code of Conduct. Now is the time to ensure that the company's Code of Conduct adequately addresses important compliance concerns, risk areas, and cultural commitments to ethics and integrity. An effective Code should be more than just words on the page, and companies should take steps to ensure that the policies and principles in the Code are effectively communicated and implemented at all levels of the organization.
6. Make workplace culture a priority. Employees who fear retaliation or do not trust their managers and corporate leaders to make ethical decisions are much less likely to come forward internally with reports of misconduct. Employers should work to promote an ethical workplace culture in which employees feel comfortable speaking up about potentially unlawful or unethical conduct.

[Earl \(Chip\) M. Jones III](#) is the Office Managing Shareholder of Littler's Dallas and Northwest Arkansas offices; [Philip Storm](#) is a Shareholder in the Chicago office; and [Amy Mendenhall](#) is a Knowledge Management Counsel in the Washington D.C. office. If you would like further information, please contact your Littler attorney at 1.888.Littler or [info@littler.com](mailto:info@littler.com), Mr. Jones at [ejones@littler.com](mailto:ejones@littler.com), Mr. Storm at [pstorm@littler.com](mailto:pstorm@littler.com), or Ms. Mendenhall at [amendenhall@littler.com](mailto:amendenhall@littler.com).