Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5 Essential Elements Of An Effective Anti-Retaliation Program

By **Roman Darmer, Shireen Matthews and Cheryl O'Connor**
(July 26, 2019, 2:49 PM EDT)

The need for companies to implement robust internal compliance programs that include an effective anti-retaliation component has never been greater.

Roman Darmer

Shireen Matthews

Cheryl O'Connor

The Dodd-Frank Act[1] incentivizes would-be whistleblowers to report alleged misconduct directly to the government in the first instance. Astounding seven- and eight-figure payouts to whistleblowers by the U.S. Securities and Exchange Commission and the Commodity Futures Trading Commission are the new norm, and receive widespread media coverage.[2]

The SEC is commencing enforcement actions against companies whose policies allegedly limit the ability of employees to report alleged misconduct outside of the company. And juries are demonstrating a willingness to return substantial verdicts to whistleblowers based on claims of unlawful retaliation.

On April 30, the U.S. Department of Justice released an updated version of its guidance document, Evaluation of Corporate Compliance Programs, highlighting factors it considers important when evaluating the effectiveness of a compliance program for purposes of charging and settlement decisions.[3]

Importantly, the DOJ guidance notes that if a compliance program identifies misconduct, allowing for timely remediation and self-reporting, a federal prosecutor should view the occurrence as a strong indicator that the company's compliance program was working effectively. This means that it is critical for a company to facilitate internal reporting of employee and whistleblower concerns in the first instance.

While there is no single road map for a successful compliance program, there are several key elements that can be incorporated into an effective anti-retaliation program at every company.

Refocus the Company's Whistleblower Approach From Reactive to Proactive

The most effective way to prevent retaliation in the workplace is to refocus a company's approach to employee concerns and whistleblower complaints as opportunities to resolve issues before they develop into bigger problems, rather than as problems to be avoided.

Recent research indicates that companies with stronger internal-reporting systems experience fewer bad outcomes measured in terms of lawsuits and settlement amounts.[4] The opportunity to obtain valuable information about the root cause of a problem before it is disclosed publicly or to a government agency enables a company to address potentially serious misconduct in the first instance, including any necessary remediation, and allows the company to make its own determination as to whether self-reporting or other responses are warranted.

Develop Clear Anti-Retaliation Policies Reinforced by Senior Management

Managing employees to achieve any business objective is much easier when the goal is clearly articulated and understood by all personnel necessary to accomplish the task. Developing a culture of compliance that exhibits zero tolerance of retaliatory conduct is no different. While it may seem obvious, a key step a company can take is to ensure that its compliance documents, including its anti-retaliation policy, are clear, concise and consistent with applicable federal and state laws.[5]

At a bare minimum, this must include a robust code of ethics, employee handbook and anti-retaliation policy written in plain English that clearly identifies retaliation against whistleblowers as misconduct that is unlawful and will not be tolerated. Ideally, a company's policies will make clear that compliance concerns raised by employees are welcome, and explain the process the company will follow in response to any expressed concerns, including concerns about retaliation.

In order to be effective, an anti-retaliation program needs to be regularly and visibly supported by senior management as well as the board of directors.[6] Where possible, management should consider public recognition, as well as other incentives for employees whose disclosure of suspected misconduct led to improvements or changes that benefited the company.

Implement Transparent and Accessible Ways for Employees to Report Concerns Internally

One of the key takeaways from the literature on whistleblower motivation is that most employees do not want to harm the company, and that external reporting is often a last resort.[7] Therefore, a company must make it as easy as possible for employees to report internally.

A company may provide multiple channels, including a hotline, email address or third-party website for receipt of anonymous tips, as well as a designated company official or ombudsman responsible for receiving and processing any concerns. Whatever process is implemented, it must not restrict or limit employees from reporting concerns or complaints outside the company to the government or oversight agency.

Likewise, however a concern or complaint is received, a company must ensure it is timely and fairly reviewed at the appropriate level of the company, the board or by outside counsel, depending on the nature of the issue.

Conduct Training and Retraining on the Anti-Retaliation Policy at All Levels

Effective and targeted training of all managers and supervisors is critical to the success of a company's anti-retaliation policy.[8] It is vital that each manager understand the many forms that retaliation can take in order to prevent it.

Anti-retaliation training should be provided at an accessible level, using language that is easily understood by the intended audience. The training should cover (1) the company's anti-retaliation policies; (2) federal and state anti-retaliation laws, including federal and state whistleblower protection laws; (3) employee rights and obligations to report concerns or misconduct; and (4) the substantial consequences for companies found to have violated those laws.

Each manager and supervisor should come away from the training fully informed about the company's zero tolerance for retaliation, as well as the consequences for managers who fail to follow the company's anti-retaliation policies or respond to employee concerns inappropriately.

Anti-retaliation training and retraining is critical because the types of adverse actions that can amount to retaliation as a matter of law can sometimes be difficult to recognize and remediate. Therefore, a robust anti-retaliation training will also cover the types of actions, by themselves or taken together, that can amount to retaliation.

Such actions range from overt actions — such as terminations, demotions, changed job descriptions and denial of overtime or advancement — to common but more subtle behaviors — such as excluding, intimidating, belittling an employee's expressed concerns or making false accusations of poor performance.

Effective anti-retaliation training will also specifically address how a manager or supervisor should respond to a direct or indirect report of a workplace concern by any employee, including employee confidentiality issues, the process and language to use in responding to such a concern, and the obligation to report any expressed concern or complaint within the company.

Additional or refresher training should be a regular part of a company's anti-retaliation program at least annually, or as often as needed based on changes in the law, events within the company or as a result of program oversight, which we address below.

Conduct Testing and Oversight of the Anti-Retaliation Policy

The essential question for any anti-retaliation program is: "Does it work?"[9] While this can be a difficult question to answer in the absence of complaints or claims of retaliation, rigorous program oversight must be a routine feature of a company's anti-retaliation program.

Oversight methods can include monitoring and auditing. Monitoring is typically an internal analysis by the company of whether the anti-retaliation program is achieving the company's goals.[10] Auditing refers to a systematic review of a company's anti-retaliation program conducted by individuals with relevant experience who are independent of the program. For example, audits of a company's anti-retaliation can be done by an internal audit department.

Program oversight tools can include anonymous surveys of employees, focus groups of personnel to determine perceptions of the workplace environment and how management responds to raised concerns, and confidential interviews of employees who have reported compliance concerns or retaliation.

The results of program oversight should be reported directly to the board and used as a basis for ongoing evolution of the anti-retaliation program. If the results of program oversight are inconsistent with other relevant sources of information, such as grievances or complaints made by employees to outside agencies or in exit interviews, the company should consider how it engages with employees on the issue and whether changes in training or policies are necessary.

Finally, the board should consider requiring regular reports from management measuring the effectiveness of the company's entire compliance program, including the anti-retaliation component, to ensure that the company remains self-critical in its approach, and to ensure that the program is continuously modified and improved as necessary.

Conclusion

An anti-retaliation program is successful when managers follow the program's policies and employees bring any concerns about potential misconduct to the company in the first instance. Given the financial and other incentives for employees to report their concerns outside of the company, companies that make it easy and safe for employees to report their concerns by implementing an effective anti-retaliation program are much more likely to be the first to learn about a potential problem.

Roman Darmer, Shireen Matthews and Cheryl O'Connor are partners at Jones Day.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 111-203, 124 Stat. 1376 (codified as amended in scattered sections of 7 U.S.C., 12 U.S.C. and 15 U.S.C.).

[2] Office of the Whistleblower, SEC, Whistleblower Program, at 9–11 (2018); CFTC, Annual Report on the Whistleblower Program and Customer Education Initiatives, at 2–4 (2018).

[3] Criminal Division, U.S. Dep't of Justice, Evaluation of Corporate Compliance Programs, at 1 (Apr. 2019), https://www.justice.gov/criminal-fraud/page/file/937501/download.

[4] Stephen R. Stubben & Kyle T. Welch, Evidence on the Use and Efficacy of Internal Whistleblowing Systems 3–4 (January 2019), http://www.utah-wac.org/2019/Papers/stubben_UWAC.pdf.

[5] See U.S. Dep't of Justice, Evaluation of Corporate Compliance Programs, at 3–4.

[6] See id. at 9–10.

[7] See Ethics Resource Center, National Business Ethics Survey of the U.S. Workforce at 30 (2014), https://www.ibe.org.uk/userassets/surveys/nbes2013.pdf.

[8] See U.S. Dep't of Justice, Evaluation of Corporate Compliance Programs, at 4–5.

[9] See id. at 13–14.

[10] See id. at 14–15.