NAVEX GLOBAL®
The Ethics and Compliance Experts

WHITE PAPER

Modern Whistleblower Retaliation Risk Require a Modern Framework

By Matt Kelly, CEO, *Radical Compliance*

If compliance officers ever needed one more sign about the importance of anti-retaliation programs, it arrived on September 29, 2016.

On that day, the Securities and Exchange Commission (SEC) fined a company that makes casino equipment $500,000 for allowing an employee to suffer whistleblower retaliation, without any underlying misconduct having occurred. The company had investigated the employee's allegations and found them baseless. But because the employee was then fired, on those grounds alone the SEC imposed its penalty as allowed under the Dodd-Frank Act.

In other words, a company isn't liable for whistleblower retaliation only when an employee points out misconduct and suffers for speaking up; a company can be liable whenever an employee suffers for speaking up, period.

That enforcement action is the logical conclusion to a string of decisions about whistleblower protections—which, taken altogether, should make all corporate compliance officers pause and reflect. Clearly whistleblower and anti-retaliation risks are rising; anyone can see that now. But due to the nature of this rise, our response can't simply be to roll out anti-retaliation training twice as often, or to brief the board about retaliation complaints twice as much.

Consider the SEC's new attention to "pre-taliation" in employee agreements. Consider the proliferation of anti-retaliation statutes in countries like Britain, France and elsewhere. Consider the eight-figure rewards some whistleblowers now receive when they go to regulators with tales of trouble. That isn't increased whistleblower risk; that is a new type of whistleblower risk all together.

As a compliance officer, you need to contemplate the framework you use to manage this evolving breed of risk. You need to review, and possibly reconfigure, all the tools and tricks at your disposal to have whistleblower anti-retaliation programs that work in today's environment. This is no easy task.

Modernize Your Thinking

The change in retaliation risk can be found in three enforcement actions we've seen this year:

- A distribution company fined $265,000 in June for the pre-taliation risks embedded in its employee contracts
- A $3.5 million whistleblower reward the SEC announced in May, with the amount partly determined based on other companies blacklisting the whistleblower after he left his firm
- The above-mentioned stand-alone enforcement action, where the company was liable even though the whistleblower's allegations weren't valid

The common theme across all three examples? The companies' liability stemmed at least in part from a corporate culture that worked to thwart whistleblowers, rather than from misconduct that actually did happen. (Indeed, in our third example, misconduct wasn't involved at all.) The critical element was simply a culture that felt retaliatory.

That's the shift in thinking that compliance officers need to make. We need to view whistleblower retaliation risk as a problem of culture to be adjusted—not a problem of actions that need to be stopped.

Some compliance officers might say they already understand that change—and yes, at a conceptual level, the challenge is easy to grasp. But we still need to take that pause mentioned earlier. We need to step back and re-examine all the tools, concepts and frameworks that compliance officers have at their disposal, and ensure we are using them as effectively as possible now that the nature of whistleblower risk has changed.

Modernize Your Tactics

Your tactics in response to modern whistleblower risk fall into two categories: the control environment and control activities.

Let's start with an example. If a risk is rooted in flawed corporate culture, the importance of tools and controls that affect culture become more important. So you need to step back and ask: Are the CEO and other senior leaders willing to talk about anti-retaliation more often? Can we include examples of discipline for retaliation offense in the company newsletter? Me personally, the chief compliance officer—do I have enough influence with the CEO and HR department so those ideas are considered seriously?

If we wanted to place that above paragraph somewhere in the COSO framework for effective internal control, we would say it fits in the control environment: the standards and structures that provide the basis for carrying out internal control. This is where principles like strong tone at the top, commitment to ethical conduct, and holding people accountable all reside.

So what about training, hotlines, investigations—are they still important? Absolutely. These are the control activities that work within the control environment. These are the specific tools and procedures you use to enforce your compliance program. They can work even without a strong control environment, but they won't work as effectively.

To put things another way, the shift in how regulators treat whistleblower retaliation has increased the importance of a company's control environment. Compliance officers need to craft a program based on that reality. Thankfully, most large companies already understand the basic control activities you need: the hotlines, the training, the investigation protocols and so forth. But they will never resolve your whistleblower retaliation risks unless the company's control environment conveys to everyone that whistleblowing is welcome.

Recall the NAVEX Global 2016 Ethics & Compliance Training Benchmark Report released in May 2016. That report asked compliance officers what they believed undermines compliance training efforts. The top result (at 37 percent, among 12 choices) was employee cynicism that corporate culture won't really change.

A mismatch between the control environment and control activities is where employee cynicism comes from. If you have a strong environment but weak activities, employees start thinking, "We talk a good game but never really stop this problem." On the other hand, if control activities are strong but the environment is weak, they think, "We go through all the motions, but nobody at the top really cares."

Middle Management: The Connective Tissue Between Environment and Activities

Once we start thinking about retaliation risk as a problem of the control environment, the solutions become more clear. In fact, the COSO framework for internal control has five specific principles that demonstrate a strong control environment, and at least three directly apply to retaliation risk:

- The organization demonstrates a commitment to integrity and ethical values
- The organization demonstrates a commitment to attract, develop and retain competent individuals in alignment with objectives
- The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives

If your CEO and board are serious about fostering a speak-up culture and cracking down on retaliation, the compliance officer should be able to take any of the three principles mentioned above and say, "Here's how we achieve this principle for the objective of no whistleblower retaliation."

Again, all that theory is easy to grasp—but we're still missing something. Compliance officers need to take all this attention and deliver it to the place in their enterprise where it will have the most impact.

That point in the enterprise is, of course, middle management.

Middle managers are the connective tissue between senior executives setting the control environment, and frontline employees who experience the control activities. These are the people who can tell senior executives (including you, the chief compliance officer) whether the control environment is too weak, or which control activities don't work.

For a culture-based risk like whistleblower retaliation, where the effectiveness of your compliance program hinges on everyone believing the words the CEO and board put forth (in the Code of Conduct, employee memos, or anywhere else), the support of middle managers is essential. Your anti-retaliation program will not succeed without them.

That means the chief compliance officer must ask constantly: How does middle management perceive our control environment? How does our control environment address retaliation risk and how do middle managers respond to that?

That kind of thinking opens up new lines of inquiry about your policies and procedures—which are, really, just the manifestation of the control environment you want to have. For example, if the company wants to hold people accountable for the goal of anti-retaliation, you'll want to explore how compensation goals are tied to an anti-retaliation culture (or how compensation penalties are tied to retaliatory acts). If the company wants to demonstrate a commitment to the ethical value of anti-retaliation, you'll want to explore how often the CEO discusses it with the workforce or how easily employees can use your whistleblower hotline.

All of this gets you closer to a more modern, more useful assessment of your whistleblower retaliation risks. The risk isn't "We let acts of retaliation happen" or "We don't have necessary tools like a whistleblower hotline." The risk is whether or not your culture impedes a whistleblower's ability to raise concerns. So your compliance program needs to engage that risk where it lives: in your control environment, and through your middle managers who connect the control environment to your control activities.

A Word on the Practical

None of this talk about the control environment should diminish the importance of control activities. Every company needs a whistleblower hotline, ideally in multiple languages. Every company should have an investigations protocol, so it can respond quickly and systematically to whistleblowers who raise allegations.

That said, let's not delude ourselves: plenty of companies have whistleblower hotlines and investigations, and still suffer from retaliation complaints all the time. All those practical tools won't serve a compliance officer terribly well if the corporate culture doesn't take whistleblower retaliation seriously, and the control environment is what shapes corporate culture.

We could even go as far as to say the regulators are ahead of the curve here: they've already decided to define whistleblower risk as an issue of corporate culture. Hence their crackdown on pre-taliation clauses and on retaliation without any actual misconduct having occurred. Does your company impede a whistleblower's ability to speak up about misconduct? That's the question that regulators want to unravel when they hear about whistleblower retaliation.

You as a compliance officer do have the frameworks and tools to answer that question, and then to fortify the weak spots in your culture and compliance program. The journey might take some imaginative thinking compared to past exercises in anti-retaliation compliance, but a more holistic treatment of whistleblower retaliation risk is an idea whose time has come.

ABOUT THE AUTHOR

Matt Kelly, CEO, *Radical Compliance*

Matt Kelly was editor of Compliance Week from 2006-2015. Prior to his role at Compliance Week, he was a reporter and contributor on corporate compliance and technology issues for magazines such as Time, Boston Business Journal, eWeek and numerous other publications. Matt now maintains his own blog, Radical Compliance, and writes and speaks frequently on all things GRC. Follow him at @compliancememe or email him at mkelly@radicalcompliance.com.

ABOUT NAVEX GLOBAL

NAVEX Global's comprehensive suite of ethics and compliance software, content and services helps organizations protect their people, reputation and bottom line. Trusted by 95 of the FORTUNE 100 and more than 12,500 clients, our solutions are informed by the largest ethics and compliance community in the world.