The U.S. Securities and Exchange Commission is more active and aggressive in enforcement than ever. Last year it brought a record 755 enforcement actions and obtained orders totaling $4.16 billion in disgorgement and penalties. While the post-financial crisis brought a temporary shift in enforcement priorities, the SEC has a renewed focus on investigating and bringing more public-company accounting and disclosure cases. And, it is effectively using a new tool to bolster those enforcement efforts—paying whistleblowers.

The SEC began its whistleblower program four years ago pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. In short, if an individual voluntarily contacts the SEC and provides “original information” about a possible federal securities law violation, and the information leads to a successful enforcement action with a monetary sanction of more than $1 million, the whistleblower is eligible for a bounty of between 10 and 30 percent of the collected sanction.

To date, the SEC has paid out more than $50 million to 17 whistleblowers and has pronounced its desire to make bigger awards and to do so more frequently. There are few exclusions on who is eligible to receive an award. Under certain circumstances, a recipient can even include a company’s own lawyers, accountants, and compliance personnel. In fact, the SEC recently awarded about $1.5 million to a compliance officer who tipped the SEC about a violation by the officer’s own company.

Unfortunately, whistleblowers don’t have to first report internally to be eligible to receive an SEC award, although the SEC says doing so could result in a bigger award. The fear that many companies have is getting blindsided by an SEC investigation of conduct never reported internally. When reported internally, a company has the opportunity to control the situation by investigating the potential misconduct and, when needed, remediating the issue and self-reporting to appropriate authorities. Indeed, companies who detect, remediate, and self-report misconduct can receive less severe sanctions under policies of the SEC and other agencies. Beyond governmental leniency, there are other benefits to companies who can handle misconduct on the front end, including limiting the monetary and reputational fallout after the violations are publically disclosed.

While a company is prohibited from doing anything that might prevent a whistleblower from reporting potential misconduct to the SEC, there’s plenty that companies can do to encourage internal reporting. The good news is that the vast majority of employees who made reports to the SEC first reported the misconduct internally, and often multiple times. Here are some do’s and don’ts to managing an effective internal whistleblower program.

### 1. Do set the right tone, at the top and middle.
Actions speak louder than words. Every organization must communicate its own guiding values and principles. But, it’s critical that management act consistently with those written and spoken values and principles because employees always notice when there’s a gap between what is said and what is done. “Tone at the top,” i.e., senior management, is imperative because it filters down throughout the organization, but it’s equally important that the right tone is set by middle management, with whom employees interact most. Companies cannot expect employees to act differently than those in charge.

### 2. Don’t ignore internal reports or fail to properly investigate them.
Companies should have an established process to properly investigate reports of both...
potential misconduct and retaliation. The process should be in the company’s written code of conduct or, if separate, its whistleblower policy. And that process must be followed when there’s a report. A demonstrated process to address internal reports is absolutely necessary to foster the trust in potential whistleblowers that their concerns will be taken seriously and handled appropriately.

3. **Do mandatory training for employees and managers of the company’s written whistleblower and anti-retaliation policy.** Companies need a written whistleblower and anti-retaliation policy, either as a stand-alone policy or as part of its code of conduct. The SEC whistleblower law includes broad anti-retaliation provisions, which the SEC is aggressively enforcing. The policy needs to clearly explain to employees and other stakeholders 1. their duty to speak up; 2. the various ways in which they can make a report; 3. that there is no tolerance for retaliation and the consequences if it occurs; and 4. the type of behavior which constitutes retaliation. The standards and expectations established in the policy need to be set out to employees in mandatory, periodic training. Studies show that employees most often make reports to their immediate supervisor or another manager who they believe can address their concerns. Indeed, direct reports to management often points to a healthy compliance culture. Therefore, managers need to be separately trained on how to handle reports of possible misconduct, as well as recognizing potential retaliation and how to respond.

4. **Don’t forget the need to regularly communicate.** First, organizations should regularly reinforce the principles contained in their code of conduct, as well as the need to speak up about potential misconduct and its anti-retaliation policy. This is a process outside of training where the company can gain invaluable feedback about employee perceptions. Second, companies need to designate someone to liaison with an internal whistleblower, providing regular status updates and assurance that the report is being taken seriously, and to receive concerns about retaliation. This is a critical step where many organizations stumble. The less an employee perceives that her concerns are being taken seriously internally, the more likely the employee will make a report to a third-party, like the SEC.

Matthew G. Nielsen is a partner in Andrew Kurth’s Corporate Compliance, Investigations and Defense practice group in Dallas. His practice focuses on defending SEC and other government investigations and proceedings, conducting internal investigations, and defending civil securities litigation.