Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Whistleblowing

Another Record-Breaking Year In the Making?

An e-Book publication sponsored by THE Network Integrated GRC Solutions

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has quickly become one of the most important go-to resources for public companies; Compliance Week now reaches more than 26,000 financial, legal, audit, risk, and compliance executives.

THE Network
Integrated GRC Solutions

The Network is a leading provider of integrated governance, risk and compliance (GRC) solutions that prevent, detect and remediate misconduct to help companies maintain ethical cultures. The Network's solutions include our industry-first Integrated GRC Suite with advanced reporting and analytics, whistleblower hotline reporting programs, Code of Conduct and full library of engaging ethics and compliance training and awareness programs. Our solutions, ethics and compliance expertise and commitment to customer success helps more than 4,000 customers and half of the Fortune 500 identify and mitigate risks every day. For more information visit http://www.tnwinc.com and follow our industry leading Twitter feed at @TheNetworkInc.

Inside this e-Book:

Whistleblower Program's Latest Threat

By Karen Kroll

Corporate compliance officers may have a new reason to be uncomfortable with the Securities and Exchange Commission's whistleblower program: how well it appears to be working.

The whistleblower program developed by the Securities and Exchange Commission may be one of a handful of government programs that receives mostly favorable marks from those who interact with it. "The office is becoming the gold standard," says Stephen Kohn, executive director of the National Whistleblower Center in Washington D.C.

When the program was first announced, compliance executives feared that whistleblowers could bypass internal reporting mechanisms and take concerns directly to the SEC. Companies fretted that the first time they could find out about a problem is when the SEC comes knocking at the door. Based on the volume of tips flowing to the SEC, those fears look to be substantiated.

The SEC's Office of the Whistleblower, created by the Dodd-Frank Act, opened its doors in August 2011, and since then the SEC has received nearly 10,200 tips, and the volume keeps rising. In fiscal year 2014, which ended in September, it fielded 3,620 tips, up nearly 12 percent from 2013.

Several attributes distinguish the SEC's efforts from whistleblower programs in other agencies, observers say. It has built a reputation for dealing fairly and promptly with whistleblowers. It has gone to court to protect whistleblowers from retaliatory measures. And it has issued awards to individuals in other countries, as well as those with compliance responsibilities.

"The SEC has institutionally embraced the whistleblower statute," says Brian Kenney, senior partner with Kenney & McCafferty, a Philadelphia-based law firm focused on whistleblower cases. "They encourage whistleblowers and their advocates" and engage in relatively open exchanges.

The number and magnitude of the awards it pays out have also jumped. Nine of the 14 whistleblower awards issued to date occurred in fiscal 2014, including a $30 million award issued in September. In addition to being the largest so far, that was the fourth award to a whistleblower living in a foreign country.

The magnitude of the awards "really emphasizes the need for companies to invest in compliance programs," says Robert Wild of Krieg DeVault in Chicago. The eye-popping payments it has made to some whistleblowers also provides incentives employees need to come forward, he says. "Fifty thousand dollars isn't enough for people to risk their careers."

Motivation From Madoff

The SEC's current receptivity to whistleblowers may have its roots in the Commission's failure to uncover the Ponzi scheme perpetrated by Bernard Madoff for more than a decade. An investigation by the SEC's Office of Inspector General concluded in part, "the SEC received numerous substantive complaints since 1992 that raised significant red flags concerning Madoff's hedge fund operations … although the SEC conducted five examinations and investigations of Madoff based upon these substantive complaints, they never took the necessary and basic steps to determine if Madoff was misrepresenting his trading."

"It was a lot of embarrassment," but gave the SEC a strong incentive to develop an effective whistleblower program, Kenney says.

Among the features of the program that aid whistleblowers is the SEC's focus on preventing retaliation. Rule 21F-17 from the SEC prohibits anyone from taking "any action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement." "This limits companies' abilities to hide behind confidentiality agreements," says Kyle Eisenmann of the law firm Kenney & McCafferty.

Moreover, the SEC can bring action against organizations that retaliate or impede investigations. In 2014, the Commission pursued its first such case when it fined Paradigm Capital Management $2.2 million after the firm stripped an anonymous whistleblower of his or her job functions.

The SEC has also argued to the courts that anti-retaliation measures should protect both individuals who report to the Commission as well as those who report internally within their organizations. In his letter in the 2014 report, Chief of the SEC's Office of the Whistleblower Sean McKessy notes that refusal to provide this protection could encourage individuals to forego their companies' internal compliance programs.

The international reach of the whistleblower office also is a positive, Kohn says. "The office understands that violations of U.S. securities law can occur in other countries." According the SEC's report, it has accepted claims from individuals in 88 countries. The largest numbers have come from Canada, India, and the United Kingdom.

How Does It Stack Up?

Many of those who work with multiple whistleblower programs rank the SEC's initiatives at the tops of their lists. While the SEC receives praise for its overall receptiveness to whistleblowers, for example, the IRS has been criticized for ignoring them.

Writing in Politico recently, Sen. Ron Wyden (D-Ore.), chair of the Senate Finance Committee, and Sen. Chuck Grassley (R-IA), said: "We've been puzzled why the IRS often snubs whistleblowers who may provide invaluable evi-

dence of wrongdoing, especially when the costs of inaction are only growing … We routinely hear from whistleblowers who complain about how the IRS handles their cases. They are strung along for years without any indication that the IRS is even looking into their claims. Others are flat-out ignored."

While the SEC's whistleblower program has garnered plaudits, that's not to say it hasn't come in for criticism. Connecticut lawyer Harold Burke questions the small number of awards paid out relative to the number of tips received—just fourteen awards from ten thousand tips. "A lot have been filed, but how many are turning into something?" he asks. At the same time, he acknowledges that insider-trading cases can take years to investigate and prosecute.

Indeed, the SEC's program dwarfs the first few years of awards after the False Claims Act was strengthened in 1986, Kohn points out. Awards for the first four years, through 1991, totaled about $18.8 million. In contrast, the SEC paid at least $32 million in whistleblower awards during the first nine months of 2014 alone.

The small number of awards helps protect the program's "long-term trajectory," says Geoffrey Rapp, law professor at the University of Toledo. If the SEC's whistleblower office had issued hundreds of awards its first year, the momentum would have been difficult to sustain. Rapp does question the fact that awards are only issued once the penalties collected exceed $1 million. This overlooks the fact that many victims of fraud are smaller, he says.

Kohn says the awards should include claims submitted before Dodd-Frank went into effect in 2010. The SEC has interpreted the law to cover only information received after July 2010, despite no date of eligibility being stated in the law itself, he says, adding this is being challenged in court.

Some observers would like more transparency to the program. They argue that having greater detail on the cases would enable other companies to check they're not making (perhaps inadvertently) the same kinds of mistakes.

Others say safeguarding the identity of whistleblowers takes priority. "What I do find great is that the SEC is committed to protecting the identity of whistleblowers," says Jessica Tillipman, assistant dean with the George Washington University Law School. "They often risk their jobs and livelihoods."

Rapp notes that if it was possible for outsiders to identify the organizations paying whistleblower awards, they might then be able to infer the individuals who brought forward the claims, putting them at risk. The SEC is "doing their best to satisfy multiple goals," he adds.

One big question is how the program might change down the road. "These things are political footballs," Burke says. A new administration could shift policy and direction and diminish the whistleblower office's power and enforcement activities.

For now, many of those working with the program express satisfaction with the way in which it's been developed. "Whistleblowers feel they're getting a fair shake from the SEC," Kenney says. ■

INCREASE IN WHISTLEBLOWER TIPS

Below is a look at the amount of whistleblower tips the SEC has received since the inception of its Whistleblower Office.

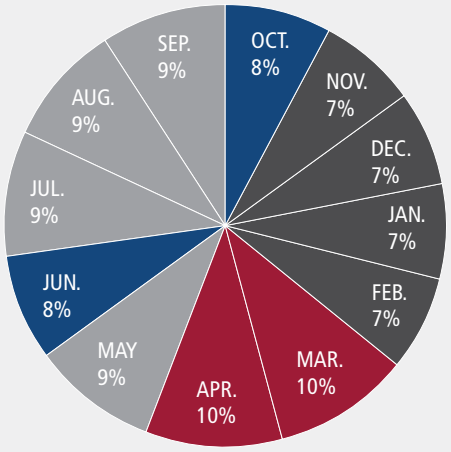
For each year that the whistleblower program has been in operation, the Commission has received an increasing number of whistleblower tips. Since August 2011, the Commission has received a total of 10,193 whistleblower tips, and in Fiscal Year 2014 alone, received 3,620 whistleblower TCRs.

The table below shows the number of whistleblower tips received by the Commission on a yearly basis since the inception of the whistleblower program:

FY2011	FY2012	FY2013	FY2014
334	3,001	3,238	3,620

As reflected in the table, the number of whistleblower tips received by the Commission has increased each year the program has been in operation. From Fiscal Year 2012, the first year for which we have full-year data, to Fiscal Year 2014, the number of whistleblower tips received by the Commission has grown more than 20 percent.

The chart below shows by percentage the number of whistleblower tips the Commission received on a monthly basis during Fiscal Year 2014. As reflected in the chart, the volume of tips remained relatively steady throughout the year, with the highest number of whistleblower tips being received during the months of March and April.



Source: SEC.

Whistleblower Protections Expand

During fiscal year 2013, the SEC saw an uptick in whistleblower complaints and last year, the agency issued a $14 million award

By Jaclyn Jaeger

With more whistleblower complaints coming in to agencies like the SEC, more regulators adding rules to protect corporate whistleblowers, and a recent Supreme Court decision that expands whistleblower protections to employees of private companies, it's becoming apparent that all companies need to do more to address whistleblower retaliation risks.

Companies must contend not only with whistleblower protections included in the Dodd-Frank Act and Sarbanes-Oxley Act, but also with courts and regulators that continue to widen the scope of whistleblower protections. "There is a confluence of factors that is contributing to this uptick in whistleblower claims," says Steve Pearlman, a partner in the labor and employment law department of law firm Proskauer.

Whistleblowers flooded the Securities and Exchange Commission, for example, with 3,238 tips and complaints during fiscal year 2013, up from 3,001 during the same period 2012. And with last year's record $14 million award, more informants are likely to come forward in coming years.

It's not just public companies that now have to worry about establishing whistleblower protections. In March, the U.S. Supreme Court ruled in *Lawson v. FMR* that the Sarbanes-Oxley Act prohibits not just public companies from retaliating against their employees for engaging in protected whistleblower activities, but also the private contractors of those public companies. The decision means that many private companies are now subject to Sarbanes-Oxley whistleblower claims, which could be problematic since most don't have proper anti-retaliation compliance controls in place.

The good news is that companies have the ability to reduce the likelihood of a whistleblower claim by avoiding the common cultural pitfalls that get them into trouble in the first place. A good first step is to have in place a code of conduct and an anti-retaliation policy, but it doesn't stop there; nor does it stop with having in place an open-door policy that simply encourages employees to speak up.

"Everybody has an open-door policy," says Heather Sager, a member of the labor and employment group at law firm Vedder Price. The more important question is what happens after an initial complaint is made, even if that complaint is baseless, she says.

Complicating matters is that most employees who engage in protected whistleblower activity are, quite often, individuals who have reason to believe their employment may be in jeopardy. "I've seen many instances where an employee goes into a termination meeting with a very good idea of what's coming, and all of a sudden raises a complaint," says Martha Zackin, a partner with labor and employment law firm Bello Welsh.

> "I've seen many instances where an employee goes into a termination meeting with a very good idea of what's coming and all of a sudden raises a complaint."
>
> Martha Zackin, Partner, Bello Welsh

Employees commonly presume that whistleblower protection laws create "a *de facto* get-out-of-jail-free card, where employers will be more hesitant to take adverse employment action following their protected activity," Sager says. While that's not necessarily the case, companies must still use extreme caution in how they handle the claim. Documentation is critical in such cases, so employers can show the adverse action they take with an employee is not related to a whistleblower claim.

Other employees who commonly launch complaints may have a beef with their boss, or don't get along well with their coworkers—all traits that make it tempting to dismiss a whistleblower's allegations.

This is an area where companies commonly open themselves up to an anti-retaliation claim, because many managers and supervisors mistakenly assume that retaliation can't take place where a legitimate concern hasn't been raised.

"Whistleblower protections, however, are not dependent on whether a concern is justified, or results in an actual legal violation," Sager warns. Furthermore, it's not always the whistleblower who creates the liability, as much as it is the operational managers who work with the employees on a day-to-day basis and make decisions in response to that protected activity, she says.

For this reason, managers and supervisors should take every complaint seriously, and look into them when they're reported. "They'd need to do an investigation," advises Sager.

Standard Procedures

Companies also need to have in place "an established procedure for dealing with employee concerns that are raised," says Stephen Berry, partner and chair of employment law at law firm Paul Hastings. "Follow-up with those employees to let them know the outcome of the investigation and let them know what actions were taken."

When reports are made and not addressed, it sends a message to employees that their concerns are not being taken seriously, says Zackin. That then makes it much less likely that employees will make reports going forward, opening the company up to potentially even greater liability.

"You always have an inherent risk of a rogue manager responding inappropriately to a whistleblower complaint," says Pearlman. In those situations where retaliation does occur, it's crucial that the company reacts swiftly, effectively, and in a very transparent way to address the situation. "Determine whether and to what extent discipline is appropriate," he says.

Firms further should document their measures to be able to show the actions they took. "If you can show that you have a complaint-reporting procedure that's communicated to employees and encourages them to report wrongdoing, and you have an effective policy for handling reports of non-compliance, and that the complaint has been investigated, than you're going to have a much higher probability of defeating a whistleblower claim," says Berry.

Training is another important way to let management know retaliation will not be tolerated, and that management sees the value in encouraging whistleblowing. Pearlman recommends "having a higher-level executive present, at least at the very beginning of the training, to show that the company takes anti-retaliation seriously."

In addition, frontline managers and supervisors should be trained to recognize where the land mines are, what constitutes a formal complaint, and the right and wrong way to respond to concerns.

"There may be confusion about whether a complaint needs to be in writing, or whether it can be oral, or whether the complaint needs to be made to a certain specific person," says Zackin. "It's important that there is some structure to the process, but that it's not so rigid that certain types of complaints are excluded."

By having a robust and effective internal complaint process coupled with a culture that rewards ethical behavior and penalizes wrongdoing, Zackin says, "the company stands on much better footing, and is in a much better position to defend itself, if a complaint is made externally." ■

RELATED CONTENT

In SEC News…

The SEC issued a sizable whistleblower award to a former corporate officer. The SEC stated that while corporate officers and directors are typically not eligible under the Dodd-Frank whistleblower statute to receive awards, the statute carves out an exception if an officer reports information concerning misconduct to the SEC more than 120 days after other responsible compliance personnel at the company possessed the information and failed to adequately address the issue. The award was the first issued to a corporate officer by the agency under that exception.

McKessy

The SEC awarded the corporate officer between $475,000 and $575,000 for information that resulted in a successful enforcement action. Andrew Ceresney, Director of the SEC's Division of Enforcement, stated that the officer in question "should be commended for stepping up to report a securities law violation when it became apparent that the company's internal compliance system was not functioning well enough to address it."

> "Companies must have rigorous internal compliance programs that adequately address and remedy potential violations voiced by their employees as well as by their officers, directors, or other individuals."
>
> Sean McKessy, Chief, SEC's Office of the Whistleblower

Sean McKessy, Chief of the SEC's Office of the Whistleblower, added that the case demonstrated that "companies must have rigorous internal compliance programs that adequately address and remedy potential violations voiced by their employees as well as by their officers, directors, or other individuals."

In August 2014, the SEC announced a similar type of award to a whistleblower employee who was in the internal audit and compliance areas of a company. In that case, the employee reported wrongdoing to the SEC after the whistleblower's company failed to take action when the whistleblower reported it internally. The SEC noted that the August 2014 award was the "first award for a whistleblower with an audit or compliance function at a company."

Bruce Carton

Embracing Whistleblowers

Understand the Real Risk and Cultivate a Culture of Reporting

When most compliance practitioners think about whistleblowers, the last thing they think about is embracing them. After all, whistleblowers cost companies millions in fines, penalties, and legal fees and upend your life as a compliance professional. In a moment of frustration or anger, it is easy to imagine whistleblowers with a big smile on their face, waiting for a big payday under Dodd-Frank and gleeful at the cost and chaos they have caused.

But are they?

There are certainly whistleblowers whose intentions are questionable at best. However, the reality is that most whistleblowers are often simply trying to do the right thing and more likely than not tried to report their concerns to their companies long before they ever went to a government regulator. While it may seem unthinkable when you are in "the crisis," one of the best ways to manage whistleblower risk is to understand and embrace whistleblowers, and most importantly to take their concerns seriously.

Show Me the Risk

It's not a reach to question whistleblower motivations. In September of 2014, the SEC awarded more than $30 million to a whistleblower, an amount that was more than double the next highest award.[1] With such potential payouts it's easy to imagine a long line of employees waiting to turn snitch. Indeed, the SEC even awarded a half million dollars to a corporate officer turned whistleblower this year.[2]

Aside from the hard money costs, the damage a single SEC inquiry can cause is significant, regardless of whether or not the claim ends up being substantiated. The sheer cost of time and labor required to produce documents alone is staggering, not to mention hiring additional legal support, reputational costs, etc.

Given all of this, it's also easy to think of whistleblower bounty programs as some kind of perverse practical joke. After all, the government first requires or incents you to put together a compliance program and then appears to pay people to circumvent it. Working in compliance certainly isn't for the faint of heart.

The first step in managing a risk is to understand it. Whistleblowers are not some juggernaut waiting to undo everything you are trying to achieve in compliance. For example, it's worth noting that the SEC has authorized awards for only fourteen whistleblowers in the history of the program. The statistics for 2014 are even more daunting for whistleblowers. In 2014, the SEC received 3,620 tips, but authorized just 9 awards to whistleblowers.[3]

It also turns out that financial incentives are not actually the primary motivator for external reporting. New research from the University of North Carolina reports that the primary reason whistleblowers go outside the company is a fear of retaliation—not a desire to cash in on bounty programs.[4] This supports earlier findings that monetary incentives are the least likely motivator of external reporting.[5]

Still, even if the barbarians are not at the gate, the risk is still real and potentially costly. You need a strategy that is effective, sustainable, and consistent with your values as an ethical organization.

Let's examine why that strategy should include embracing this person who has just upended your life as a compliance professional.

The Average Whistleblower Isn't Who You Think

Managing the risk requires employers to understand who whistleblowers are and what motivates them … and they might not be who you think they are.

Many seasoned compliance professionals and senior leaders will tell you with confidence that whistleblowers are most likely to be disgruntled employees out to get revenge for some perceived wrongdoing. However, data show that they are wrong. The average reporter is likely to be an actively engaged, well-performing employee, most likely a supervisor or higher-level manager.

1 2014 Annual Report to Congress on the Dodd-Frank Whistleblower Program, http://www.sec.gov/about/offices/owb/annual-report-2014.pdf

2 SEC Gives Former Officer $500,000 Whistleblower Award, Wall Street Journal, http://blogs.wsj.com/riskandcompliance/2015/03/02/sec-gives-former-officer-half-million-dollar-whistleblower-award/?cb=logged0.872530589113012

3 2014 Annual Report to Congress on the Dodd-Frank Whistleblower Program, www.sec.gov/about/offices/owb/annual-report-2014.pdf

4 Internal Corporate Whistleblowers Swayed by Protections, Not Pay: Study, Insurance Journal, http://www.insurancejournal.com/news/national/2015/03/03/359116.htm

5 Inside the Mind of a Whistleblower, http://www.ethics.org/files/u5/reportingFinal_0.pdf

Most importantly, the average whistleblower is someone who most likely went to the company first. A staggering 92 percent of reporters turn to somebody inside the company when they first report misconduct.[6] Only 20 percent of reporters ever tell someone outside their company of their concerns, and only 9 percent of employees report to the government. That means you have a chance to uncover and address the vast majority of potential issues before regulators, the media, or lawyers ever get involved.

Many seasoned compliance professionals and senior leaders will tell you with confidence that whistleblowers are most likely to be disgruntled employees out to get revenge for some perceived wrongdoing.

However, the fact that whistleblowers may prefer to keep things in the company doesn't mean they won't turn to the government or media if they think it necessary. Sixty-five percent of surveyed employees would be willing to report externally, "if my company didn't do anything with my internal report." An even higher percentage would report externally, "if keeping quiet would cause possible harm to people" or "if it was a big enough crime."[7]

One other consideration is retaliation. One in five whistleblowers experienced retaliation after internally reporting misconduct.[8] For a frame of reference, that's 6.2 million people. Retaliation not only impacts the reporting party—but sends a powerful message to other employees. Indeed, just over 1 in 3 employees who declined to report a problem pointed to a fear of payback from senior leadership as the primary reason they stayed out of things.[9]

The net result? Far from discouraging whistleblowing, retaliation drives employees into the arms of investigators—and makes it less likely that you will learn of a problem while there is still time to address it internally. That is why recent research suggests that "companies that want to encourage internal reporting of wrongdoing should focus on developing and implementing anti-retaliation policies to protect whistleblowers."[10]

… But Wait, There's Another Whistleblower Risk

One other thing to know about whistleblowers: They might not work for your company. Indeed, one in five whistleblowers are the consultants and contractors you hire.[11] This underscores the importance of making sure your internal reporting procedures are communicated to your extended enterprise, and, depending on the particular circumstances of your organization, published on either your investor relations page or a publicly available ethics and compliance page on your website.

This also highlights the importance of having adequate resources to communicate and train your extended enterprise regarding your reporting options. You should consider a Supplier Code of Conduct and make sure it provides suppliers with the information and guidance they need to use your internal reporting resources. Your contracts too should address the need to report concerns directly to the company. Finally, you should consider providing training for your third-party partners. While the cost and effort necessary to train third parties may be daunting, you should at least consider providing training on critical topics like your Code, ethical decision making, and high-risk areas like anti-bribery.

6 National Business Ethics Survey, http://www.ethics.org/downloads/2013NBESFinalWeb.pdf

7 Inside the Mind of a Whistleblower, http://www.ethics.org/files/u5/reportingFinal_0.pdf

8 National Business Ethics Survey, http://www.ethics.org/downloads/2013NBESFinalWeb.pdf

9 National Business Ethics Survey, http://www.ethics.org/downloads/2013NBESFinalWeb.pdf

10 Internal Corporate Whistleblowers Swayed by Protections, Not Pay: Study, Insurance Journal, http://www.insurancejournal.com/news/national/2015/03/03/359116.htm

11 2014 Annual Report to Congress on the Dodd-Frank Whistleblower Program, http://www.sec.gov/about/offices/owb/annual-report-2014.pdf

The Best Defense Is a Good Offense – Embrace a Culture of Reporting

What can you do to manage the risk? For most organizations, encouraging a speak-up culture (and ensuring it permeates your extended enterprise) is the most effective way to manage potential whistleblower liability—and the one factor entirely within your control. A strong reporting culture will not only make sure you learn about potential problems, studies show it will actually lead to a decline in misconduct.[12]

How do you build a strong ethical culture and encourage internal reporting?

1. **Engage senior leaders: Talk means nothing if senior leaders don't take ethics and compliance seriously.**

You're probably tired of hearing about tone from the top, but that doesn't make it any less effective or important. Your employees' perception of a senior leader's ethics depends upon three primary factors:

a. The overall character of the leader, as experienced through personal interaction

b. How the leader handles crises

c. The policies and procedures the leader issues and adopts to manage his organization[13]

The fact is that employees look to leaders as role models who set the tone for the entire organization. This extends to your senior leaders' conduct outside of work. Leaders who practiced 24-7 integrity were correlated with a stronger employee commitment to ethical conduct and greater employee engagement.[14] These trends will only accelerate given the continuing rise of social media, mobility, and the blurring between public and private matters.

2. **Give middle managers tools and training they need to support your ethics and compliance initiatives.**

Middle managers are a critical but often overlooked and under-supported part of the solution. While nearly 70 percent of employees will report an incident to their direct supervisor, only 58 percent of managers feel prepared to handle employee reports of misconduct.[15]

To close this gap, you need to provide middle management with the support and guidance they need. First, make sure you train them on your Code and other critical risk areas. Middle managers can hardly be expected to address potential reports if they cannot spot the importance of the issue being reported.

Second, you should make sure that middle managers understand how to report an issue brought to them by an employee. While hotline and Web-based reporting mechanisms are familiar to many employers, many have not yet embraced leadership or "walk up forms." These Web-based forms allow managers to document incidents that employees have brought to them, feed directly into your incident management system, and allow you to document and report on investigations.

Finally, and perhaps most importantly, you need to provide managers with training around how to have ethics- and compliance-related conversations. They may or may not know how or what to document, who to give it to, and what kind of incident reports meet your escalation criteria. The closeness and trust that employees feel toward their immediate supervisors makes these middle managers the ideal people to carry the message of ethics and compliance with authority.

3. **Create and publicize a quality hotline reporting program.**

Hotline programs have been around for years, but are more important than ever in today's regulatory and business environment. Compliance teams should stop thinking of hotlines as purely telephonic; they've grown to include mobile and Web-based reporting solutions that give employees and others a safe and reliable way to raise their concerns internally via whatever method is most comfortable for them. They also give the compliance team important insight into what is going on inside the company.

Hotline reporting programs are complex and there is a lot more to write on this topic, but keep four things in mind:

1. Reporting programs are only effective if your employees

12 National Business Ethics Survey, http://www.ethics.org/downloads/2013NBESFinalWeb.pdf

13 Ethical Leadership: Every Leader Sets a Tone, http://www.ethics.org/nbes/wp-content/uploads/2014/12/ExecSummaryLeadership.pdf

14 Ethical Leadership: Every Leader Sets a Tone, http://www.ethics.org/nbes/wp-content/uploads/2014/12/ExecSummaryLeadership.pdf

15 Risk Intelligence Quarterly, Q1 2014, CEB, http://ceb.uberflip.com/i/256261/25

know they exist, when to use them, and what to expect. Effective communications are a critical part of program success.

2. Don't just sit there, do something. Nearly 60 percent of those who did not report cited a belief that the employer would not act on their concerns as reason for not reporting, while more than 80% of employees who called the hotline reported a belief that the employer would act as their reason for calling.[16] Make sure you have processes in place to investigate and resolve concerns. Many hotline providers have incident management solutions that will ensure reports don't fall through the cracks.

For most organizations encouraging a speak-up culture (and ensuring it permeates your extended enterprise) is the most effective way to manage potential whistleblower liability—and the one factor entirely within your control.

3. Educate employees about what happens when they file a report, so they understand the process and how reports will be investigated. Removing the mystery and fear surrounding the process will reinforce the perception that your company takes reports seriously.

4. Quality matters. Even in today's digital age, word of mouth is the second most common way your people learn about your hotline. A quality experience will communicate your commitment to hearing your employees' concerns. A bad experience undercuts everything you are trying to achieve.

For a more in-depth view, take a look at our Comprehensive Guide to Ethics and Compliance Hotline Reporting Programs.

4. **Communicate the value your organization places on acting ethically in the workplace. Use a layered approach using different communication and training tools.**

Experienced compliance professionals will tell you that there is really only one way to effectively minimize the cost and disruption of a government investigation or lawsuit: avoid it in the first place. To do that, you need to provide your employees with the information and guidance they need to make good decisions.

A good training and communications program is layered and leverages different avenues to reach employees. Don't forget how quickly people become blind to messages they see frequently. Advertisers call this phenomenon "ad blindness". This same phenomenon affects us in compliance in that we face a similar battle with keeping our compliance communications fresh in our employees' minds.

5. **Train managers on what constitutes retaliation and why it matters.**

When it comes to whistleblowing risk, retaliation represents a triple threat:

- It creates potential liability for employers, even when the underlying complaint is unfounded.
- Most managers fail to understand retaliation and how to avoid it.
- Fear of retaliation is strongly correlated with whether or not an employee will report internally.

Preventing retaliation starts with having a speak-up culture, but that's not enough. Create, communicate, and enforce an anti-retaliation policy, and remember it's especially important to train managers. Managers can only avoid or report retaliation if they know what retaliation looks like.

In Conclusion: Make Lemonade.

Whistleblowers represent a real risk to your organization, and that risk needs to be addressed. However, most whistleblowers are often simply concerned employees. Embrace the idea of the whistleblower as the motivator for making your ethics and compliance program as strong as it can be, rather than as an enemy out for revenge. Create the culture and provide

16 Inside the Mind of a Whistleblower, http://www.ethics.org/files/u5/reportingFinal_0.pdf

How Companies Silence Employees

By Joe Mont

In June, the Securities and Exchange Commission took its first-ever enforcement action against a company for whistleblower retaliation. The next agenda item for the SEC, as it lays down the law regarding the treatment of potential whistleblowers, may be a crackdown on non-disclosure agreements.

Companies of all sizes, across many industries, require employees to sign confidentiality agreements that prohibit them from discussing anything about their former employer. A tech giant, for example, doesn't want the specs of its new tablet leaked throughout the Internet; a hedge fund wants to retain a competitive advantage by protecting its investment strategy. Non-disclosure agreements, however, are increasingly used as a tactic to discourage whistleblowers from going to the government and, in the case of SEC tips, collecting a bounty.

Among the companies under scrutiny for having whistleblower-silencing confidentiality demands is Kellogg, Brown and Root, a Halliburton subsidiary and defense contractor. The SEC is investigating its use of these agreements. The company recently lost a legal bid to classify such agreements under the umbrella of attorney-client privilege.

A *Washington Post* report found that International Relief and Development, a non-profit that collected more than $1 billion in tax dollars for war-related projects, tried to silence employees from reporting to government agencies. According to the report, Stephen Cohen, associate director of the Division of Enforcement at the SEC, said: "I'm very concerned about these kinds of agreements. It is likely that a lot of people are not coming to us because of these agreements. Anything that inhibits a person's desire to come forward to tell us about violations of the law is deeply troubling."

Some corporate lawyers are growing concerned about the practice too. "We see a seemingly endless array of efforts by companies to come up with new ways to dissuade individuals from providing information to the government," says David Marshall, a partner at the law firm Katz, Marshall & Banks who specializes in whistleblower cases. "Many of them are couched in terms that look, at first blush, like they might be legitimate, but they can also be used to interfere with speaking with the government."

Others say while the agreements may say they forbid former employees from providing information to the government, they might not have much legal standing. "Companies are trying to use them, even though I don't think you could ever have a non-disclosure agreement supersede statutory law or individual rights," says Brian Dickerson, an attorney with the whistleblower-focused law firm Roetzel. "I don't see how you will get the agreements to stick."

There is no question that the SEC has the tools it needs to pursue the use of confidentiality agreements to thwart whistleblowers. In creating its bounty program, it went one step beyond the Dodd-Frank Act authorization to include the following language: "No person may take any action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement."

"That was the first time, to my knowledge, that an agency told corporations they could not use confidentiality agreements, which are routine for corporate employees, to prevent employees from speaking out," Marshall says.

> "We see a seemingly endless array of efforts by companies to come up with new ways to dissuade individuals from providing information to the government."
>
> David Marshall, Partner, Katz, Marshall & Banks

Worst Practices

The use of these agreements also runs contrary to the U.S. Sentencing Guidelines and its expectations for compliance programs, Dickerson says. "I'd hate to be the lawyer who has to go into the Department of Justice to say they are complying with the U.S. Sentencing Guidelines, which require a compliance program that is effectively implemented, and even though they have a whistleblower hotline there is also a rule that says employees can't use it. It is contrary to the intent of their own compliance program and that's what most of these companies fail at."

Some companies may be rethinking confidentiality agreements in general, given the speed and ease at which information now travels. Companies that try the confidentiality gambit may be on a fool's errand, Dickerson says. "It is old school thinking to think you can keep people quiet with so many media outlets and blogs available to them, never mind going directly to the SEC."

An example of a non-disclosure agreement that Marshall came across in one case, reads:

"[Employee] hereby irrevocably assigns to the federal government, or relevant state or local government, any right Employee may have to any proceeds, bounties or awards in connection with any claims filed by or on behalf of the government under any laws, including but not

limited to, the False Claims Act and/or the Dodd-Frank Act (and/or any state or local counterparts of these federal statutes or any other federal, state or local qui tam or "bounty" statute) against the Company. Employee also represents and promises that Employee will deliver any such proceeds, bounties or awards to the United States government (or other appropriate governmental unit)."

No-Collect Clauses

Marshall says an increasing number of companies are trying more creative tactics. "What we've seen is a lot more of companies realizing they can't include an agreement that prevents an employee from reporting information to the SEC," he explains. "Instead, they try to dissuade reporting to the SEC indirectly by trying to remove the incentive that was established in the whistleblower program."

They are doing that by demanding, carefully crafted contracts as part of severance agreements and exit interviews. "They might say that nothing in the agreement will prohibit you from providing information to government authorities or cooperating in an investigation," Marshall says. "However, in the event that you receive any compensation or award, you agree to waive it. In the event that they participate in one of these bounty programs, they have to say they won't collect."

Other clauses may require an employee to notify the company immediately if they receive any contact from a regulator or investigating agency.

Marshall compares the SEC program to a law enforcement agency's practice of posting a notice of monetary reward on the bulletin board in the post office for anyone providing information that leads to the arrest of a bank robber. "A company should not be able by contract to require a whistleblower to forego an award from the SEC any more than a bank robber should be able by contract to require members of the community not to accept an award for turning him in to the authorities in response to a wanted poster in the post office," he says, adding that he thinks a court, at some point, would find these agreements null and void.

These maneuvers are contrary to the intent of what regulators and lawmakers intended. "The idea is not to foment prosecutions of companies; it is to encourage compliance internally so things don't have to be dealt with by regulators, Marshall says.

Things can be problematic, however, for companies that impose non-disclosure agreements for legitimate reasons, but fail to see the whistleblower ramifications. "We recommend that you have to, at least annually, have an audit where you have all your department heads in there, including human resources, and your compliance officer is going through everything to make sure that the policies and procedures all reflect the goal of the company," Dickerson says. "If you don't do that, this can fall through the cracks and be looked at negatively if there is an investigation."

"Nobody looks a these investigations in foresight; it is all 20/20 hindsight," he adds. "You have to think that way when you do your review." ■

AML ACTIVITY

The following, from the Department of Energy, provides an example of how government employees are notified that non-disclosure agreements should not restrict their rights as a whistleblower.

Pursuant to the Whistleblower Protection Enhancement Act of 2012, the following statement applies to every nondisclosure policy, form, or agreement of the Government (with current or former federal employees), including those in effect before the Act's effective date of Dec. 27, 2012:

"These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling."

The following executive orders and statutory provisions are controlling in the case of any conflict with an agency non-disclosure policy, form, or agreement, as of March 14, 2013:

- Executive Order No. 13526;
- Section 7211 of Title 5, United States Code (governing disclosures to Congress);
- Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military);

Source: Department of Energy.

2014 Marked Record Year for SEC Tips

By Jaclyn Jaeger

Fiscal year 2014 marked an historic year for the Securities and Exchange Commission's Whistleblower Program both in terms of the number and dollar amount of whistleblower rewards the agency doled out, according to the SEC's annual report to Congress.

"Fiscal Year 2014 was historic for the office in terms of both the number and dollar amount of whistleblower awards," Sean McKessy, Chief of Office of the Whistleblower, said in the report. "The Commission issued whistleblower awards to more individuals in Fiscal Year 2014 than in all previous years combined."

The SEC received 3,620 whistleblower tips in 2014, compared to 3,238 last year. Since its inception in 2011, the SEC has doled out awards to 14 whistleblowers, nine of which received whistleblower awards this year.

"Not only did the number of whistleblower rewards rise signficantly, but the magnitude of the award payments was record-breaking," McKessy said. This year saw the largest ever whistleblower award of more than $30 million given to a whistleblower who provided important information that led to a successful enforcement action. "The whistleblower in this matter provided information of an ongoing fraud that otherwise would have been very difficult to detect," McKessy said.

The SEC also has renewed its focus on the anti-retaliation provisions of the whistleblower regime in reaching its first settlement of $2.2 million with a company who allegedly retaliated against a whistleblower. "The Commission's action sends a strong message to employers that retaliation against whistleblowers in any form is unacceptable," McKessy said.

> "Fiscal Year 2014 was historic for the office in terms of both the number and dollar amount of whistleblower awards."
>
> Sean McKessy, Chief of Office of the Whistleblower

Consistent over the last three years, the most common allegations were corporate disclosures and financials (17%), offering fraud (16%), and manipulation (15%).

Whistleblower Profile

In an effort to be more transparent, the SEC provided slightly more details than in previous years on the profile of whistleblowers, while still maintaining confidentiality as required under the Dodd-Frank Act.

"Among many of the complaints the SEC received, for example, "the information provided by each award recipient was specific, in that the whistleblower identified particular individuals involved in the fraud, or pointed to specific documents that substantiated their allegations or explained where such documents could be located," the SEC stated. "In some instances, the whistleblower identified specific financial transactions that evidenced the fraud."

Several of the individuals who have received awards to date were company insiders; more than 40 percent of whistleblowers who received awards were current or former employees. An additional 20 percent of the whistleblowers were contractors, consultants, or were solicited to act as consultants for the company that committed the securities violation.

Of the whistleblowers who were current or former employees, over 80 percent raised their concerns internally to their supervisors or compliance personnel before reporting the wrongdoing to the SEC. The broader lesson is that companies "not only need to have internal reporting mechanisms in place, but they must act upon credible allegations of potential wrongdoing when voiced by their employees," McKessy stated in the report.

The SEC received tips through other channels as well. "The remaining award recipients obtained their information because they were investors who had been victims of the fraud, or were professionals working in the same or similar industry, or had a personal relationship with one of the defendants," the SEC stated.

Geographic Scope

During Fiscal Year 2014, the Commission received whistleblower submissions from individuals in all fifty states, as well as from the District of Columbia and the U.S. territory of Puerto Rico.

Within the United States, the majority of complaints, by far, came from California, at 556 complaints. The second highest number of complaints (264) came from Florida, followed by Texas and New York, with 208 and 204 complaints, respectively.

"It's important for multinational corporations to be aware that this is far from an exclusively U.S. issue," John Warren, senior associate of law firm Freshfields, said. "The SEC has an ever-expanding geographic reach, with tips received from 60 different countries."

Outside the United States, the bulk of whistleblower tips came from the United Kingdom (70), India (69), and Canada (58). The fourth and fifth highest number of tips was received from whistleblowers in the People's Republic of China (32) and Australia (29). ■

The Largest Ever Whistleblower Bounty

$30 million notable informant award will incentivize whistleblowers around the world, says Chief of the SEC's Office of the Whistleblower Sean McKessy

By Joe Mont

With its largest ever whistleblower bounty, the Securities and Exchange Commission awarded $30 million to an informant whose tips led to a major enforcement action. The previous high for an SEC award to a whistleblower was $14 million, which was announced in October 2013.

The award is also notable because it is the fourth award to a whistleblower living in a foreign country. "This award of more than $30 million shows the international breadth of our whistleblower program as we effectively utilize valuable tips from anyone, anywhere to bring wrongdoers to justice," Sean McKessy, chief of the SEC's Office of the Whistleblower, said in a statement. "Whistleblowers from all over the world should feel similarly incentivized to come forward with credible information about potential violations of the U.S. securities laws."

The SEC's whistleblower program rewards "high-quality, original information" that results in an SEC enforcement action with sanctions exceeding $1 million. Awards can range from 10 percent to 30 percent of the money collected in a case. The money paid to whistleblowers comes from an investor protection fund established by Congress that is financed through monetary sanctions paid by securities law violators to the SEC. By law, the SEC protects the confidentiality of whistleblowers and does not disclose information that might directly or indirectly reveal a whistleblower's identity.

Because of the program's anonymity protections, no details regarding the enforcement action that led to the reward were made public.

"Our client exposed extraordinarily deceitful and opportunistic practices that were deeply entrenched and well hidden," Erika Kelton, an attorney with the law firm Phillips & Cohen and legal counsel to the whistleblower says. "Federal regulators never would have known about this fraud otherwise, and the scheme to cheat investors likely would have continued indefinitely."

"I was very concerned that investors were being cheated out of millions of dollars and that the company was misleading them about its actions," the whistleblower said in a statement issued through the firm. "Deception had become an accepted business practice."

A Costly Delay?

Without divulging specifics, the Commission suggested that the whistleblower's initial delay in reporting the uncovered malfeasance limited the award that will be collected.

"We have considered Claimant's delay in reporting the violations, which under the circumstances we find unreasonable," the administrative order says. "The Claimant delayed coming to the Commission after first learning of the violations, during which time investors continued to suffer significant monetary injury that otherwise might have been avoided. We do not agree with Claimant's assertion that the delay was reasonable under the circumstances because [he/she] was purportedly uncertain whether the Commission would in fact take action. There is always some measure of uncertainty about how a law- enforcement agency may respond to a tip, but in our view this does not excuse a lengthy reporting delay while investors continue to suffer losses."

> "Our client exposed extraordinarily deceitful and opportunistic practices that were deeply entreched and well hidden."
>
> Erika Kelton, Attorney, Philips & Cohen

"Indeed, if the Claimant was concerned that the Commission would not respond to the tip, [he/she] also could have reported the violations to other appropriate U.S. authorities; yet Claimant did not do so and the explanations offered are not sufficient to mitigate a downward adjustment," the SEC added.

A mitigating factor, however, was that a good portion of the delay occurred before the Comission's whistleblower bounty award program was established by the Dodd-Frank Act.

"Although Claimant has not raised any specific legal arguments against application of the unreasonable delay factor for that portion of the delay, we have determined in our discretion not to apply the unreasonable delay consideration as severely here as we otherwise might have done had the delay occurred entirely after the program's creation," according to the administrative order. ■

Create a Better Workplace.

Whistleblowers have the potential to cost companies millions in fines, penalties and legal fees and upend your life as a compliance professional. A speak-up culture is the most effective way to manage potential whistleblower liability – and the one factor entirely within your control.

Protect your employees, your reputation and your bottom line, with confidence and security.

Detect and prevent ethics and compliance issues using a comprehensive, collaborative approach.

Correct risk issues across the enterprise and connect compliance with performance.

Gain valuable insight into your ethics and compliance initiatives, across your entire enterprise, with the Integrated GRC Suite from The Network.

grc 20/20 Technology Innovator 2013

www.tnwinc.com | 1.800.253.0453

THE Network
Integrated GRC Solutions