COSMOS
Navigate the Compliance Universe

CEP Magazine - February 2023

Scott Moritz (scott.moritz@whitecollarforensic.com) is President of White Collar Forensic LLC in New York, New York, USA.

How to get the most out of your confidential hotline

By Scott Moritz, CFE

Organizations are expected to have investigative capabilities, yet the majority do not. In fact, the U.S. Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) consider confidential reporting and internal investigation to be among the most critical hallmarks of an effective compliance program. A very important initial step toward meeting the government's compliance program expectations is starting a hotline. There is a lot more to this hallmark than retaining a software provider and deploying their platform.

In its publication *Evaluation of Corporate Compliance Programs*, the DOJ builds on its prior guidance to emphasize the importance of an "efficient and trusted mechanism by which employees can anonymously or confidentially report allegations . . ."[1]

Consistent with other DOJ-published guidance, it is written from the perspective of how prosecutors should go about assessing the compliance programs of defendant companies.

For example, it states: "Prosecutors should assess whether the company's complaint-handling process includes proactive measures to create a workplace atmosphere without fear of retaliation, appropriate processes for the submission of complaints, and processes to protect whistleblowers. Prosecutors should also assess the company's processes for handling investigations of such complaints, including the routing of complaints to proper personnel, timely completion of thorough investigations, and appropriate follow-up and discipline."

The *Evaluation of Corporate Compliance Programs* document poses many questions about hotlines and investigative processes, including:

- "Does the company have an anonymous reporting mechanism and, if not, why not?"
    - Implementing one or more anonymous reporting mechanisms usually becomes an obvious choice. It has either been pointed out to the organization that they are of a size, complexity, and geographic diversity that it would be appropriate to implement them, or one or more significant matters went unreported because there was no obvious reporting channel. If the organization has decided against implementing reporting mechanisms, it is essential to document the thought process underlying that decision and for the company to be prepared to defend that position.
- "How is the reporting mechanism publicized to the company's employees and other third parties? Has it been used?"
    - Having a hotline that no one knows about and is never used raises many concerns about the effectiveness of other key elements of the compliance program, including training and

communications, program oversight and governance, commitment by senior and middle management, investigation of misconduct, and the overarching question: "Does the Corporation's Compliance Program Work in Practice?"

- "Does the company take measures to test whether employees are aware of the hotline and feel comfortable using it?"
    - Retaliation is very real and is often the number one reason people don't speak up. Gauging employee and manager awareness of confidential reporting channels and their comfort level using them can be an excellent watermark of the state of the company's ethical culture; it can focus leadership on the extent to which culture must be improved.
- "How has the company assessed the seriousness of the allegations it received? Has the compliance function had full access to reporting and investigative information?"
    - While these questions are meant to assist prosecutors in evaluating compliance programs, compliance personnel would be well-advised to use them to critique themselves and the state of their program. Once you have a hotline in place, heightened obligations and expectations attach. One way to test the overall effectiveness of the confidential reporting channels and investigative processes is for internal audit to regularly assess the process from end to end and pose some of the same questions raised in the DOJ's guidance.

Tactical considerations

A lot of what goes into standing up and staffing a hotline is anticipating what *could* happen and providing hotline personnel with guidance on how to respond. The decision to implement a hotline and/or other confidential reporting channels was very likely preceded by numerous incidents and allegations requiring investigation. Studying those incidents will help you conceptualize your hotline incident response and investigative process and who should be involved. It will also help determine how to decide what alerts progress to larger investigations, how investigations should be performed and documented, and the criteria governing disciplinary actions. Below are some of the main activities associated with effective hotlines and investigative processes.

Triaging

Alerts tend to fall into one of several categories, which then dictate what part of the organization should oversee the investigation and the skill sets that will be required. In most instances, alerts might be grouped as follows: human resources (HR), internal audit, cyber, privacy, compliance, legal, corporate security, or the audit committee. Not all organizations have all these functions, but you get the idea. For example, if an alert comes through the hotline that a branch manager has been verbally abusive to his colleagues and direct reports, that is probably best routed to HR. Any written guidance intended to assist company personnel in properly routing alerts for review should include examples of the different types of alerts that are anticipated.

Assessing an alert

Some alerts or allegations are clearly stated and detailed and include supporting documentation. Others include allegations of unknown reliability. Still others don't include enough detail to allow recipients to act on the information. In the latter scenario, many hotlines provide the ability to communicate with the whistleblower by either leaving a message for them to retrieve or through some other means. Asking specific follow-up questions can then make it possible to perform follow-up procedures.

Limited-scope investigations

Once there is enough detail in hand, and a decision has been made to perform a limited investigation, the investigative procedures should be targeted around attempting to corroborate what has been alleged. For example, if it has been alleged that the plant manager of a manufacturing facility is accepting kickbacks from specific vendors and he appears to be living beyond his means, that would suggest specific investigative steps, such as a background investigation of the plant manager and some of the vendors and a review of the recent payments to those vendors. If the background investigation reveals that the plant manager has multiple homes, several luxury vehicles and appears to have the same last name as several vendors, you probably have enough of a basis to expand the investigation. If the limited investigation does not yield anything to corroborate the allegations, document what was done and get approval to close the investigation with no further action. Ensure all investigative activity is documented in some database or repository and can be produced years later if necessary.

Full-scope investigations

If the limited investigation corroborates the allegations or the initial allegations are specific and serious, both scenarios suggest the need for a more comprehensive investigation. Full investigations often entail resource-intensive activities such as forensic accounting, imaging of computers, smartphones, and tablets, electronic discovery and analysis of email and electronic evidence, witness interviews, and background investigations. Often, organizations retain outside counsel at this point since there is an increased likelihood of the need to engage with law enforcement and regulators and make public company disclosures.

Assessing capabilities and filling gaps

Most organizations do not have all the resources needed to perform an in-depth, internal investigation. Understanding the organization's investigative capabilities and limitations is of critical importance. For instance, if your in-house legal department employs a former prosecutor, that individual is an obvious choice to lead an internal investigation. Similarly, the corporate security, cyber, or financial investigation units probably include people with law enforcement backgrounds who can play a substantive role. Inventorying these individuals and their skill sets will enable you to determine what things can be handled using these internal resources and where there are gaps. Most commonly, things like computer forensics, electronic discovery, background investigations, and forensic accounting are skill sets needed infrequently and don't exist in-house. If that's the case, it may be wise to identify outside service providers and put contracts in place to provide those services on short notice. Timely response to allegations can be the difference maker in a successful investigation. Negotiating service provider contracts before you have a need will better position the company to respond quickly should a rapid response be necessary.

The need for written policies and procedures

Internal investigations sometimes result in backlash, including wrongful termination or discrimination litigation. Creating investigative policies, procedures, and guidelines to assist company personnel and their outside service providers will enable the organization to respond consistently. Indeed, it is imperative that each employee or officer be treated fairly and equally throughout the investigation and for disciplinary actions to be meted out consistently regardless of the person's seniority or importance to the organization. Without written policies, procedures, and guidance, it is much easier for opposing counsel to support an argument that the investigative and disciplinary processes were applied inconsistently and unfairly.

Consider the culture

Investigations can be very disruptive and harmful to individual reputations. Think through the logistics of how an investigation should be performed, by whom, and even where. Internal investigations often require the support of audit, HR, and IT personnel. With each person brought into the inner circle, the likelihood of the existence of the investigation becoming common knowledge increases.

Also, when it comes time to perform more overt investigative steps such as witness interviews, think about where the interviews should be conducted and by whom. Marching someone through the offices into an all-glass conference room in the main reception area can be a humiliating experience and extremely harmful to individual reputations and organizational culture. Not every person interviewed is a subject. In fact, most interviews of individuals are for information-gathering purposes.

Internal messaging is vital because once the existence of the investigation becomes known, the rumor mill runs wild, and the anxiety level soars. Internal communications to reassure people that their jobs are not at risk and the company is in good financial health (assuming that's an accurate statement) can help alleviate the stress from the investigation and limit the inevitable gossip and conjecture. Consider conducting interviews away from public view out of respect for people's privacy and in deference to their reputations. If some witnesses are members of a labor union, there may be restrictions on how interviews can be performed and whether individuals can request that their shop steward or other union representative sit in on the interview.

Evaluate your resource needs

A big part of the rationale supporting the deployment of a hotline and other reporting channels is encouraging an increase in confidential reporting. While the increase in activity is a positive development, it can also put a drain on your existing resources. Each alert that comes through must be triaged and then routed to the appropriate group within the company for assessment and possible investigation. The designated recipient will then need to determine what steps need to be performed and by whom. Most in-house groups, such as compliance, legal, HR, cyber, internal audit, privacy, security, and investigations, run very lean and an unexpected influx of hotline alerts can be disruptive. That is why additional personnel resources should be allocated to address alerts, perform limited-scope investigations, and coordinate the activities of outside service providers. Since it is difficult to predict additional workflow, some organizations opt to engage with outside firms to help handle the overflow from the expected increase in activity evaluating alerts and performing investigations, at least until the company can better gauge what their steady state needs are likely to be.

Investing in the company's future

Implementing a hotline and upgrading and formalizing your investigative capabilities is one of the most critical steps in your organization's progression toward its goal of having an effective compliance program. It is the bedrock of your program, sets the organizational tone, and is one of the most visible indicators of the hallmark: commitment of senior and middle management. It also sends an important message about accountability and organizational ethos.

Takeaways

- The Department of Justice has increased its focus on whether you have an "efficient and trusted mechanism by which employees can anonymously or confidentially report allegations…."
- Having a hotline that no one knows about raises the question: "Does the Corporation's Compliance Program Work in Practice?"
- A consistent approach to investigations and institutional justice doesn't happen without planning.

- Not having written investigative policies, procedures, and guidance can lead to unintended consequences and liability.
- The investigative plan should consider disruptions to business operations, individual privacy, potential for reputational harm, and the risk of negatively impacting organizational culture.

1 U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, updated June 2020, https://www.justice.gov/criminal-fraud/page/file/937501/download.