COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2023
Hotline and Whistleblowing Reporting Mechanisms

By Shon C. Ramey, Esq.[1]

Overview

Hotlines are one of the most effective and cost-efficient external mechanisms that a corporation can deploy in its compliance program. This solution has been used by companies for more than 40 years. Depending on the size and complexity of an organization, hotlines also have been adopted by companies in the past decade as a best practice for fraud detection and to promote the integrity and compliance of an organization.

Various legislative initiatives have increased the use of hotlines, including the U.S. Sarbanes–Oxley Act of 2002 (SOX) and the United Kingdom's Public Interest Disclosure Act (PIDA), which came into force in the United Kingdom in 1999. As a response to several high-profile corporate scandals, SOX implemented reporting requirements for accounting and audit matters of public companies (each audit committee shall establish procedures for "the receipt, retention, and treatment of complaints received by the issuer" as well as "confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters").[2] The establishment of external hotlines satisfied the legislative requirements. Similarly, the U.S. Securities and Exchange Commission (SEC) adopted rules to create a whistleblower program of its own. As announced by the SEC on May 25, 2011,[3] the SEC whistleblower program, created under Section 922 of the Dodd–Frank Act, "rewards individuals who provide the agency with high-quality tips that lead to successful enforcement actions." Awards are available to individuals who voluntarily provide original information to the SEC that results in a successful enforcement action in which the SEC obtains sanctions totaling more than $1 million.

The SEC has awarded more than $1 billion to whistleblowers since the inception of the program. Awards started out relatively modest early in the program's history but have gotten progressively larger. In October 2020, the SEC announced its largest award of $114 million,[4] which was slightly larger than a $110 million award in September 2021.[5] Similarly, Britain created PIDA after inquiries into several major disasters revealed that dangerous conditions had persisted at certain companies for many years, and employees didn't feel there was a mechanism to address the conditions or that their concerns would be acted upon. PIDA created protections for persons who might disclose such information. British employers, keen to keep such disclosures internal and avoid prosecution under PIDA, introduced internal hotlines to receive reports of dangerous practices. The passage of SOX in the US served as a catalyst for various federal agencies to assess internal controls and reporting and response consistency to reports of improprieties. This resulted in encouragement to have whistleblower solutions by the U.S. Office of Government Ethics' internal mandate under 5 C.F.R. § 2635.101(b) and by requirements or encouragements such as the Hatch Act, the Whistleblower Protection Act, the Federal Employee Protection of Disclosures Act, and OMB Circular A-123.

Hotlines have become viewed as cheap insurance against fraud, waste, and abuse; corporate malfeasance; health and safety; harassment and other human resources–related issues; and equal employment and affirmative action claims. According to the most recent *Report to the Nations* by the Association of Certified Fraud Examiners (ACFE), the median loss for all cases across 125 countries was $125,000 per case, with the average loss per case

being approximately $1.5 million per case.[6] Obviously the longer a fraud persists, the more financial damage it causes the company. With the average duration of a fraud being 14 months from commencement to detection, the early detection or prevention of fraud can pay for the hotline and case management operations for many years. The ACFE found that 43% of all fraudulent schemes were detected by a tip, with half of those tips coming from employees. Hotlines were used by whistleblowers in 33% of all cases reported.

Hotlines should not be viewed as a primary, or even initial, means of prevention or detection of illegal, unsafe, or detrimental practices. Within most organizations, reports of malfeasance or misconduct should first be made to the employee's supervisor or an internal department (human resources, legal, compliance, etc.), and the hotline should be the final reporting option or a safe haven if anonymity is required. Employees and managers should be trained on a company's ethics and compliance requirements, usually through a code of conduct or similar document.

Additional training needs to reinforce a company's commitment to ethics and compliance while ensuring complaints are not mishandled or downplayed. Furthermore, the training should make clear that attitudes and conduct that undermine a commitment to ethics and compliance are not tolerated, and ethics and compliance are strongly backed by senior leaders and the board of directors. Unfortunately, because of the emphasis placed on the hotline by SOX, PIDA, and other legislation, a company can place an inordinate amount of emphasis on the existence of a hotline and its ability to prevent and discover ethical and compliance breaches. The hotline is an important tool in an organization's arsenal of detection and prevention, but it should be designed to support and complement an overall issue awareness strategy.

Establishing an effective issue awareness strategy provides an opportunity to instill confidence in the corporation's desire to develop and maintain a positive culture of integrity and compliance. This value can be enhanced with transparency of the inquiry as well as an issue awareness and resolution process.

Choosing a Reporting Solution

Defining and developing a reporting solution begins with an analysis of your organizational complexity. Your organization's size, industry, operational geographies, operational style (centralized or decentralized; union or non-union; weak culture or strong culture; complexity or magnitude of programs, operations, and transactions; extent of manual processes or applications; etc.), and historical significance of risk are the primary considerations. Additional consideration should be given to the primary industry or industries you serve. Each industry has a unique set of regulatory requirements and common risk components that should be serviced by the reporting solution. Finally, your organization's risk tolerance and social responsibility goals should be factored in to ensure the appropriate level of rigor and process complexity is applied.

Hotline reports should not be limited to reports of fraud and abuse. An important aspect of any good reporting solution is the ability for stakeholders to inquire about their potential actions when confronted with an ethical dilemma or to express a concern for something they believe may be occurring. It is also important to provide feedback to the reporting stakeholder as to what they can expect from the reporting process, and if you have other reporting or support vehicles in place, where and how to use them. It is important to structure the hotline system to receive actionable reports and shift frivolous concerns or other such feedback to more appropriate venues.

The most common areas of reporting for a hotline are:

- Corruption, theft, and fraud;
- Finance and accounting concerns;

- Information or asset misuse and access;
- Customer/partner/competitor concerns, including the Foreign Corrupt Practices Act[7];
- Equal opportunity/affirmative action matters;
- Environmental, health, and safety;
- Industry-specific regulatory risks;
- Harassment and other human resources–related issues; and
- General inquiry/questions.

Given the generational dynamics of today's workforce, a hotline solution should be a combination of web and telephone intake. Regardless of the method of reporting, hotlines must be trustworthy from the potential reporter's point of view. While it is possible for organizations to consider installing a toll-free line and answer calls within their organization, it is generally not cost- or process-effective. Potential reporters, especially employees who are most likely to witness issues for which the hotline was created, often don't believe that a company-created and staffed hotline will provide a confidential forum and fear retaliation. Selection of a third-party vendor ensures 24/7/365 access and availability as well as a degree of stakeholder assurance that only comes from a third-party operator. Some organizations may desire or choose to employ an ombudsman to receive and respond to certain hotline reports. This choice is often based on the culture and makeup of the organization and can prove very effective.

The choice an individual organization makes on a reporting mechanism will ultimately depend on the culture of the organization. Those organizations with a small, tightly knit employee population may favor an approach that a larger organization would find unworkable. The opposite may also be true. Regardless of how an organization chooses to implement its hotline, its presence, objective, and guidelines must be clearly communicated to the stakeholders—employees, vendors, spouses, and customers—to ensure the solution's effectiveness. Nothing is more damaging to employees' and other stakeholders' beliefs in a hotline solution than to see complaints mishandled, downplayed, or not followed up on or attitudes and conduct that undermine a commitment to ethics and compliance. These behaviors cannot be tolerated, and senior leaders and the board of directors need to send a strong and consistent message that ethics and compliance are valued throughout the organization.

International Considerations

Multinational organizations implementing a global reporting system are faced with a special set of challenges and complexities due to the various data protection laws and cultural differences among countries. In some cases, countries have passed laws or issued rulings that appear to be at odds with anonymous reporting systems, such as those mandated by the SOX.

The Commission Nationale de l'Informatique et des Libertés (CNIL) guidelines and subsequent recommendations brought forth by Germany, Belgium, and the European Union (EU) require diligent, thoughtful application and a systematic operational thoroughness.

If your organization operates worldwide, there are a number of agencies and groups that must be considered before deploying your hotline, and the list is growing. The primary groups to consider are:

- France: CNIL

- European Union: European Data Protection Board
- Germany: Düsseldorfer Kreis
- Belgium: Data Protection Authority
- Ireland: Data Protection Commission
- Japan: Financial Instruments and Exchange Act (commonly referred to as J-SOX)
- Spain: Agencia Española de Protección de Datos/Ley Orgánica de Protección de Datos de Carácter Personal (AEPD/LOPD)
- Canada: Personal Information Protection and Electronic Documents Act

When operating a whistleblower hotline outside the United States, it is important to use the local language, and, when socializing the hotline with stakeholders, it is critical to explain the purpose and process of the hotline.

Organizations should stress anti-retaliation protections and take steps to demonstrate the solution's anonymity safeguards. When describing the hotline process, ensure stakeholders understand certain categories of personal data are outside the boundary of the hotline's reporting capabilities under EU data privacy law.

As an example, employers operating in France since 2005 are required to register their whistleblowing schemes with the CNIL. This was routinely done by self-certifying under the CNIL's Single Authorization (AU-004), which indicated that the whistleblowing scheme complied with the preestablished conditions set out in this authorization. Originally, the scope of the Single Authorization was limited to finance, accounting, banking, corruption, and compliance with Section 301(4) of SOX, which required the establishment of confidential procedures for anonymous submission of questionable accounting or auditing matters and the company's treatment of those reports. But since then, the CNIL has permitted an extension of the scope of whistleblower schemes to include reports of anti-competitive practices; compliance with the Japanese Financial Instruments and Exchange Act; and certain non-financial topics, including workplace discrimination, harassment, safety, hygiene, and environmental protection.

What gets included in these categories will vary from country to country, but examples include data relating to racial or ethnic origin, health, religious or political opinions, and criminal records. It is also important to recognize many EU countries require a formal consent by the stakeholder reporting into the hotline for this data to be used and transmitted. This consent can be easily made a part of the hotline script or online reporting tool.

In an effort to satisfy the regulations of SOX or other legislative requirements, US companies with EU-based affiliates often find themselves with information gathered in the EU. To transfer or allow access to such information by the US parent requires compliance with the EU data protection rules. Historically, organizations had enjoyed convenience and protections under, first, the U.S.–EU Safe Harbor Framework, and then later, the EU–U.S. Privacy Shield. But the EU Court of Justice ruled on July 16, 2020, that the Privacy Shield Framework is no longer a valid mechanism.[8] The U.S. Department of Commerce and the European Commission have initiated discussions to determine the possibility for an enhanced EU–U.S. Privacy Shield Framework.[9]

Binding Corporate Rules for Processors

Multinational organizations have begun to consider binding corporate rules (BCRs) as another alternative. BCRs are designed to allow multinational companies to transfer personal data from the EU to affiliates located outside of the EU in compliance with data protection requirements.

Applicants must demonstrate that their BCRs have put in place adequate safeguards for protecting personal data throughout the organization, in line with EU requirements.[10]

Establishing BCRs will keep multinational companies from having to approach each individual data protection authority separately. If you want to pursue this strategy, you will need to choose a data protection authority (DPA) to be a lead authority. The choice of lead authority depends on the location of your EU headquarters, or the area within Europe where the division responsible for global protection compliance is located.

If the lead authority is satisfied with the adequacy of the safeguards put in place in your BCRs, that authority circulates the draft BCRs to the other DPAs in Europe from which you need authorization. The lead DPA communicates any comments received and assumes the role of the lead data protection authority in facilitating the authorization process.

The main advantage of BCRs over other means of providing adequate safeguards is that, once developed and operational, BCRs can provide a framework for a variety of intra-group transfers to meet your organization's requirements. With the establishment of the BCRs comes an ongoing obligation to monitor your company's compliance with the BCRs. This approach will include regular audits and a requirement to maintain a training program for staff handling personal data.

BCRs also help companies address privacy concerns and raise awareness of data protection within an organization. This is because the company will need to consider the type of personal data being transferred and the procedures it will use to make staff aware of and in compliance with the rules. An essential part of the authorization process is a requirement that the applicant must demonstrate how staff in third countries will be made aware of the implications of processing personal data transferred from the EU.

Provided a company's BCRs are drafted widely enough, they should be able to accommodate changes in corporate structure and some variation in the types of data flow. Recipients of BCRs do not need to notify DPAs of corporate changes if such changes don't affect the authorization. BCRs, therefore, allow for significant flexibility.

Communicating the Reporting Solution

Just because you have a hotline doesn't mean people will use it. You must create a communication stream that not only asserts the existence of the hotline, but communicates its value, its objectives, and the organization's commitment. Tone from the top and publicity around the hotline via posters, wallet cards, training, and even creating YouTube videos will help assure the use and importance of your hotline.

A successful hotline solution requires the organization's commitment to maintaining a culture that promotes the prevention, detection, and resolution of instances of conduct that do not conform to law, regulation, policies, or procedures.

A good initial introduction or reintroduction to your employees would include a communication from the CEO announcing the hotline's existence, its importance to the organization's core values, and a declaration of support for its use. The most common ways to publicize the hotline would include emails, posters, brochures, wallet cards, newsletter articles, website pages, code of conduct, and training events.

Continued reinforcement by the senior management team to express their support of the initiative will be much more effective than a "one-and-done" approach. Emphasis needs to be placed on the organization's commitment to the program along with a reminder that retaliation of any sort will not be tolerated.

The CEO should make clear that not only are employees encouraged to use all of the organization's reporting

methods, but also that they are expected to use the hotline if they become aware of, or are asked to participate in, a compliance violation and feel they have no other avenue to report. Companies should view an ethics communication campaign as an advertising initiative that seeks to inspire a certain behavior within the workforce.

With multiple generations operating in the workforce now, using a combination of communication vehicles to publicize the hotline is necessary. Know your audiences and ensure that publicity for the hotline communicates your organization's appreciation and willingness to accept feedback through the hotline. However, based on your code of conduct and other policies, it can be important to reinforce the hotline as a tool in your arsenal along with other reporting options, such as your open-door policy. For large companies with employees in many different locations, one of the most effective ways to build awareness of the hotline, while reinforcing the need for open and honest dialogue, is to get line managers involved.

A recent development for hotlines is to encourage not just the reporting of unethical behaviors, but also honoring those who have exhibited ethical behavior in challenging circumstances. Remember, the hotline can be a positive tool—use it to promote and support the behavior you desire from your organization.

An important component of the hotline's operation is determining how to support the desire for transparency during the inquiry and its resolution. You must decide, most likely with the assistance of your legal department, the nature and amount of feedback you will provide to those who make reports. It is important to provide assurance to reporters that they have been heard and that you are committed to the consistent enforcement of corporate behavioral expectations. Features that may assist this effort include providing a confidential report number and password known only to the reporter, which allows them to anonymously check on the company's response to their report. This feature also gives you the ability to initially research the report and ask additional, clarifying questions, and companies should encourage the reporter to provide additional information. Additionally, never miss the opportunity to reinforce your commitment to nonretaliation for those willing to assist the corporation in its self-regulation.

Anonymous v. Confidential

While it may seem unimportant, there is a common confusion between respecting the confidentiality and anonymity of a reported incident. Anonymity relates to protecting the identity of the individual who reported the issue or event, and confidentiality relates to the protection of the reported information.

Ultimately, thinking through the data flow from initial report through distribution, escalation, and resolution is a priority when establishing your hotline. It is important to control the flow of data and ensure that implicated parties, who may be recipients of hotline reports, are removed from the review process and denied access to the report. This step ensures that if an individual is named or implicated in the report, the company has an alternate data flow, including potential escalations, to address the issues implicated in the report.

Nonretaliation

The aforementioned 2020 ACFE report found that the primary reason employees choose not to report their concerns or observations is fear of being subjected to retaliation, retribution, or harassment for reporting the concern. Therefore, a nonretaliation/nonretribution policy should be established. This policy will reassure employees who wish to report concerns through the hotline or directly through the chain of supervision or compliance department.

In most cases, training supervisors and managers is essential. Many organizations find that reports received into the reporting system can inflame and evoke a negative response from the persons in authority affected by the

report. Therefore, it is critical to train managers and supervisors so they know they are not permitted to engage in retaliation, retribution, or any form of harassment directed against an employee who reports a compliance concern.

Retaliation claims continue to be an escalating issue for companies. The US Equal Employment Opportunity Commission (EEOC) released its fiscal year 2020 (October 1, 2019–September 30, 2020) statistics regarding retaliation claims, and the total number of charges has been decreasing since fiscal year 2011. Notably, however, the percentage of charges alleging retaliation has been steadily increasing since the EEOC started tracking charges in 1997. Fiscal year 2020 saw 55.8% of the claims alleging or including retaliation.[11] The 37,632 charges alleging retaliation during fiscal year 2020 (down from 39,110 in 2019) resulted in monetary benefits to claimants in the amount of $214.9 million (up from $205.2 million in 2019), which does not include benefits obtained through litigation.

Triage, Escalation, and Investigation

Identifying those within your organization who will initially receive and review hotline reports is very significant. Equally important is the creation of standards of criteria, values, and indicators that suggest or require the escalation of reported issues.

One of the most important indicators is the nature of the reported issue. Many hotline reports are unsubstantiated and reflect the bias and unjustified frustration of the author, but most are immediately actionable. Perhaps the most important step in evaluating reports is determining which ones will need resolution. Likewise, selecting and training the individuals charged with triaging your hotline reports is perhaps one of the most important activities during your implementation process.

Once a report is received into your reporting solution, it is important to establish a procedure for responding back to the individual who submitted the report. Regardless of your hotline solution, it should enable you to respond, ask follow-up questions, and otherwise communicate with the individual making the report—whether anonymous or identified.

This follow-up can be as simple as a thank-you for reporting, but it can also be a means to reinforce your program's resolution strategy. You may want to advise the reporter whether the resolution status will be shared with them. The majority of individuals who do not trust or use the hotline express fear of reprisal and the belief that nothing will be accomplished. Responding after a report is filed helps build credibility and value for your hotline solution. But remember, it is important to have your counsel review, prior to any hotline activity, your response strategy and your anticipated response remarks.

Regardless of the level of formal case management you deploy in your solution, it is important to establish a set of steps or guidelines for bringing a matter to consistent resolution. First, set a time expectation from the receipt through the review of the reported information. Next, assign a priority for the issue or matter reported. This assignment can be as simple as low, medium, or high, or something more elaborate. As noted above, this step would be the proper time to review the case for potential escalation. A case needing escalation can require specific steps for handling, the inclusion of key personnel in the process, or the inclusion of external resources. Your escalation strategy should also anticipate the elevation of a report to the chair of the audit committee or others on the board of directors. Devising the appropriate levels of protection or urgency should be based on a combination of reported information and other criteria.

You will find that a number of cases will open and close within a short period of time—sometimes the same day. Others will take much longer, and so it is important to establish a set of stages so that the resolution process can

be designated by the case owner for tracking and measurement. Steps to take following a reported issue's resolution should include more than just checking off a box showing the case was closed. Some indication of how the case was closed must be required. Simply "closed" or "resolved" will not provide your organization with the necessary analysis data points to ultimately improve your process.

Just as you devised a series of criteria and outcomes for escalation of the issue or matter, it is equally critical (especially in a decentralized organization operating in several locations) to define the potential levels of punishment and the procedures for tagging it or titling it for case management. The analytical review of your hotline, when properly established, can be invaluable to helping formulate and improve your ongoing preventive and reactive structures.

Data Retention

While there is no accepted or mandated data retention policy for US companies, don't assume the data retention requirement for hotline data is the traditional seven years. Depending on your organization, there are a myriad variables that will affect your hotline data retention policy. For instance, if you are a multinational or non-US company, the length of retention can be as short as 60 days post resolution, unless the issue has significance to the cultural values of the organization.

The best rule of thumb for retention of reports received from the hotline is a retention/destruction policy that mirrors the retention policy for similar information received or developed by your organization (e.g., for routine information gathered, investigated, and resolved, following the organization's data retention policy. If a hotline report involves a potential EEOC violation, retain the information for the minimum required period by the applicable statute).