This Checklist outlines the key steps to take and the principal issues to consider when setting up and operating a company hotline (also referred to as an ethics, compliance, reporting, or whistleblowing hotline or helpline). It addresses tone from the top, local law considerations, selection of a hotline vendor, standard hotline functions, retaliation concerns, and hotline administration, policies, procedures, promotion, and assessment.

A company hotline (also referred to as an ethics, compliance, reporting, or whistleblowing hotline or helpline) is a core element of an effective compliance program (see Practice Note, Developing a Legal Compliance Program: Five: Internal Reporting Mechanisms (4-606-5696)). A hotline can be used to:

- Communicate important information between employees and management.
- Allow employees to report sensitive matters outside the normal supervisory channels.
- Allow employees to report sensitive matters anonymously, depending on local law.
- Provide management with valuable information that can be used to reduce risk and liability for the company.

A company’s challenge is to implement a hotline that:

- Empowers employees to identify wrongdoing and protect the integrity of the organization.
- Motivates employees to report suspected misconduct internally so they are not incentivized to first turn to regulators (see Practice Note, Whistleblower Protections Under Sarbanes-Oxley and the Dodd-Frank Act: Dodd-Frank Whistleblower Incentives (7-501-7799)).
- Assures employees that, by using the hotline, their concerns can be properly investigated and addressed.

This Checklist provides an overview of the key business and legal issues to consider when setting up and operating a hotline. While this Checklist focuses on corporate hotlines, many of the steps and issues discussed also apply to hotlines in other types of organizations.

LAY THE GROUNDWORK FOR A HOTLINE

Counsel should lay the groundwork for setting up the company hotline by taking the following preliminary steps:

- **Obtain top level support for the hotline.** A successful hotline requires:
  - the strong, explicit, and visible support of the company’s governing body (such as the board of directors or board of managers) and senior management;
  - an ethical “tone from the top” that builds a culture of integrity within the company; and
  - a commitment of resources to the implementation and maintenance of the hotline program, commensurate with the company’s size and needs.

(See Practice Note, Developing a Legal Compliance Program: Obtain Top Level Commitment and Support (4-606-5696)).

- **Consider how to integrate and coordinate the hotline with other compliance initiatives.** Best practice includes synchronizing with the company’s:
  - compliance program (see Practice Note, Developing a Legal Compliance Program (4-606-5696) and Developing a Legal Compliance Program Checklist (2-595-8085));
  - code of conduct and ethics (see Practice Note, Corporate Governance Standards: Code of Ethics or Conduct (6-501-3891) and Standard Document, Code of Ethics and Business Conduct for a Public Company (2-505-5389)); and
  - other policies, practices, and governance and risk activities (such as its investigation procedures or other reporting mechanisms; see Conducting Internal Investigations: Addressing Employee Complaints and Compliance Issues Toolkit (2-502-1874)).

- **Generate a comprehensive list of laws applicable to whistleblowers and hotlines.** Include any applicable regulatory guidance and minimum policy and reporting requirements, such as:
• Section 301 of the Sarbanes-Oxley Act of 2002 (SOX), which requires public companies to have an anonymous whistleblower system for employees to internally report concerns about questionable auditing or accounting matters (see Practice Note, Whistleblower Protections Under Sarbanes-Oxley and the Dodd-Frank Act: SOX Whistleblower Protections (7-501-7799));

• the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act), which created protections and incentives for whistleblowers (see Practice Note, Whistleblower Protections Under Sarbanes-Oxley and the Dodd-Frank Act: Overview of Dodd-Frank Act Whistleblower Protections (7-501-7799) and Dodd-Frank Whistleblower Incentives (7-501-7799));

• the Whistleblower Protection Act, which protects federal employees who report government wrongdoing (see Practice Note, Whistleblower Protections Under the Whistleblower Protection Act (W-002-8554)); and

• the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), which replaces the EU Data Protection Directive (EU Directive) when it becomes applicable on May 25, 2018. The GDPR will affect how companies can handle personal data in an internal whistleblowing program (see Practice Notes, Overview of EU General Data Protection Regulation (W-007-9580) and Corporate whistleblowing hotlines and EU Data Protection Directive: Establishing compatible codes of conduct: Working Party’s recommendations (1-366-2987), and Review Local Law Requirements).

For more examples of statutes with whistleblower provisions, see Practice Notes:

• Whistleblower Complaints Under the Occupational Safety and Health Act (8-612-0573);
• Whistleblower Complaints Under the ACA (3-524-6825); and

For more information on whistleblower protections in selected jurisdictions, see Employment and Employee Benefits: Country Q&A Tool, Question 18.

Determine the scope of the hotline. Questions to resolve include:

• who is allowed to make reports using the hotline (for example, employees only or also contractors, agents, customers, suppliers, and other business partners);

• which site locations within the organization have access to the hotline (for example, offices and other company facilities within the US only or also subsidiaries and affiliates outside the US);

• what languages are relevant to the organization’s employee population;

• whether all or only certain types of misconduct (such as fraud, theft, misuse of funds, conflicts of interest, and harassment) may be reported using the hotline (for a discussion of reporting limitations, see Review Local Law Requirements); and

• whether the company also uses the hotline as a forum for employees to submit new business ideas, recommendations for improvement, and other thoughts on corporate vision and values.

UNDERSTAND LOCAL LAWS AND CULTURE

If the company is creating a multinational hotline that is available to its subsidiaries, affiliates, and other operations outside the US, it should ensure that the hotline is:

• Compliant with local laws.

• Culturally appropriate.

REVIEW LOCAL LAW REQUIREMENTS

Local laws may affect the implementation of hotlines in several key areas, including the following:

• Data protection and data retention. The privacy and data security laws of certain jurisdictions, including those adopted by EU member states under EU Directive and the GDPR, are more stringent than US laws. These laws may require that:

  • the data collected through the hotline be limited to what is strictly necessary for the report and follow-up investigation;

  • the hotline system meet specific technical requirements for the secure handling of data collected through the hotline;

  • the retention of data collected through the hotline does not exceed specified time limits; and

  • the company clearly inform employees about how data in hotline reports is handled.

• For more information on:

  • privacy issues in the US workplace, see Employee Privacy Compliance Toolkit (W-002-2530) and Employee Privacy Laws: State Q&A Tool;

  • data protection issues in the EU, see Practice Notes, Overview of EU General Data Protection Regulation (W-007-9580), Overview of EU data protection regime (Data Protection Directive 1995) (8-505-1453), and Corporate whistleblowing hotlines and EU data protection laws (1-366-2987); and

  • privacy and data protection laws in selected non-US jurisdictions, see Data Protection: Country Q&A Tool.

• Data transfer. Some jurisdictions restrict transfers of certain information (such as personal data collected from a hotline report) outside of that jurisdiction. For example, currently to legally transfer personal data outside the European Economic Area (EEA), the company may need to:

  • self-certify to the US Department of Commerce and publicly commit to comply with the requirements of the EU-US Privacy Shield Framework (see Privacy Shield Self-Certification Checklist (W-002-7961) and Standard Clause, Privacy Shield Policy (W-002-8722));

  • include standard contract clauses in an agreement between the company from which the report originates and the data recipient outside the EU;

  • have binding corporate rules that implement adequate data privacy safeguards, adopted by the data recipient and approved by relevant data protection authorities; or

  • obtain explicit and unambiguous consent from the individual whose information is being transferred.

• For more information on data transfers outside the EU, see Practice Note, Overview of EU General Data Protection Regulation:
Cross-border data transfers (W-007-9580) and Article, Expert Q&A: EU-US Personal Information Data Transfers (W-000-8901).

**Reporter anonymity.** Some countries (such as France, Germany, the Netherlands, Portugal, and Spain):
- discourage or prohibit anonymous reporting; or
- require companies to use special precautions when processing anonymous reports (such as a preliminary examination by a sole reviewer).

**Scope of reports.** The types of reports that can be made through a hotline may be limited in different jurisdictions. For example, the scope is limited in:
- France to issues of financial and accounting, workplace discrimination, harassment, and safety and environmental protection;
- Finland, Greece, and Portugal to financial matters (such as accounting, internal accounting controls, auditing matters, bribery, banking, and financial crime); and
- Sweden to using the hotline only to report on company executives and persons in key positions.

**Registration requirements.** For example, to set up a hotline in:
- France, a company must apply to the Commission nationale de l'informatique et des libertés (CNIL), the French data privacy regulator, for authorization (see CNIL: Guideline document for implementation of whistleblowing systems (10 November 2005)); and
- Denmark, a company must register with Datatilsynet, the Danish data protection agency.

**Employee rights.** Local statutes or practices may require that the company:
- consult with its local worker representatives (such as works councils in the EU) before implementing a hotline that monitors employee conduct and can result in disciplinary action;
- distribute in the local language any materials used to introduce and publicize a hotline; and
- ensure that all persons identified in a report have the right to access information provided in the report and to correct that information.

For more information on employee rights across multiple jurisdictions, see Employment and Employee Benefits: Country Q&A Tool.

### ACCOUNT FOR CULTURAL SENSITIVITIES

In some countries, the culture and history have made whistleblowing either a sensitive subject or taboo. A multinational hotline requires careful design and implementation to address cultural obstacles, such as a:
- Lack of trust in the internal system.
- Suspicion that a hotline threatens privacy rights.
- Misguided sense of loyalty to the union or work group.
- Belief that management is not held to the same standard.
- Fear of entrapment by management.
- Fear of retaliation for whistleblowing.
- Fear of being branded a “rat” or a “snitch” by peers.

Strategies to consider in launching a multinational hotline may include:
- Implementing multiple hotlines, for example, either:
  - two hotlines, including one for Europe that complies with the strictest restraints in the region and one for the rest of the world that meets robust US best practices; or
  - an individual hotline for each jurisdiction in which the company operates, with each hotline tailored to comply with local restrictions.
- Naming the hotline a “helpline” or “guideline” to overcome the negative connotations that may be attached to the terms “hotline” or “whistleblower line” (see Article, Whistleblowing: New risks, new responses: Naming the hotline (7-520-4201)).
- Creating a two-way communication system for employees to seek advice or clarification on ethical, legal, or regulatory issues, so the use of the “helpline” is less intimidating.
- Providing alternative reporting methods to make communicating sensitive matters more comfortable for employees (for example, in some countries, web-based reporting is preferred over live telephone reporting).
- Setting up easy, cheap access to the hotline and eliminating possible hurdles for reporters (for example, internet access may be unreliable in some locations or international calls may be cost-prohibitive).
- Creating targeted hotline communications for the local audience by:
  - translating hotline interfaces, materials, and communications into the local language;
  - avoiding terms that may be viewed negatively in the local culture;
  - addressing different cultural understandings of acceptable behavior (for example, facilitation payments may violate the company’s global anti-bribery policy but be standard practice in the local culture; see Practice Note, Bribery Act 2010: facilitation payments (3-505-3360)); and
  - involving local management and personnel to promote the hotline and tailor communications and training to the local audience.

For more discussion of strategies to implement an effective multinational hotline, see Practice Note, Corporate whistleblowing hotlines and EU data protection laws: Compliance strategies for hotlines (1-366-2982) and Article, Whistleblowing: New risks, new responses: Local considerations (7-520-4201).

### SELECT A HOTLINE VENDOR

**CONSIDER OPTIONS FOR MANAGING THE HOTLINE**

The company should determine whether to manage its hotline internally, such as through its human resources, legal, or compliance department, or externally, by engaging a hotline vendor. There are several advantages to having an externally managed hotline, including:
- An external vendor may be seen as an unbiased third party and reduces the appearance of impropriety.
Dialing an external number or speaking with someone who does not work for the company may create a more comfortable environment and help assure potential callers of anonymity.

Having an external call center increases availability, consistency, and quality recordkeeping in handling calls.

The company can reduce costs by not having to hire full-time employees to provide 24-hour hotline coverage.

If the company is large or has multiple locations, a hotline vendor can manage the administrative and logistical challenges and provide more sophisticated case management, which can aid in creating an appropriate and timely response.

EVALUATE COMMON HOTLINE FEATURES

If the company has decided to engage a vendor to provide and manage the hotline, the company should compare several vendor candidates by viewing demonstrations of the hotline and evaluating the following hotline features:

- **Pricing.** Compare vendor costs and pricing models (such as a fixed annual rate based on number of employees or a variable rate based on number of hotline reports).

- **Experience and customer satisfaction.** Review the vendor’s track record and contact its references to gauge customer satisfaction with the vendor’s performance and service level.

- **Accessibility.** Confirm that the hotline is available 24 hours per day, seven days per week, 365 days per year, via both a web-based reporting system and a live telephone operator.

- **Reporter feedback.** Check if the vendor offers a two-way communication system that allows the company to follow up with or request additional information from an anonymous reporter.

- **Data security.** Evaluate the privacy and data security measures that the vendor has in place. If the hotline will also be implemented outside the US, check if the vendor meets local law requirements for handling data (see Review Local Law Requirements).

- **Country compliance functions.** For non-US hotlines, check if the hotline system triggers different reporting restraints to comply with local law depending on the jurisdiction of the reporter and where the reportable incident took place (see Review Local Law Requirements).

- **Reporting methods.** Request that the vendor offer alternative methods for reporting hotline calls to the company, including email and web-based reporting.

- **Timeliness.** Ensure that all hotline reports are sent to the company in writing within a day of receipt and all high-priority reports are conveyed immediately by telephone.

- **Language capabilities.** Check that the vendor’s language translation service and multilingual operator service can handle reports in all the languages appropriate to the company’s employee population.

- **Report management.** Ensure that the vendor has document management capabilities for storing reports, company responses, communications with the reporter, and, if desired, investigation materials.

- **Tracking tools.** Determine if the vendor provides web-based tracking and analysis and creates metrics of report information.

**Insurance.** Confirm that the provider has sufficient insurance coverage for the services provided.

**Other benefits.** Ask what other service benefits are included in the agreement, such as:

- system customization;
- hotline posters and hotline-related policy templates; and
- assistance with employee training on the existence and use of the hotline.

CUSTOMIZE HOTLINE FUNCTIONS

Once the company has selected a hotline vendor, it should create a cross-functional team (including legal, compliance, human resources, and IT personnel) to customize hotline functions with the vendor, such as:

- Designing the website for the hotline, which is usually hosted by the vendor and generally includes:
  - a compliance message from the CEO;
  - an explanation of who has access and when, why, and how to use the hotline;
  - links to the company’s code of conduct and ethics, hotline policy, and other relevant policies;
  - answers to employees’ frequently asked questions;
  - online prompts to collect incident-related information from the reporter (such as country where the reporter is located, country where the incident took place, corporate group or division of the reporter, nature of the incident, and the people involved);
  - restrictions on the types of reports that can be made, in compliance with local law (see Review Local Law Requirements); and
  - translations of content into languages appropriate to the company’s employee population.

- Developing a telephone protocol for the vendor’s call center to interview reporters and memorialize telephone reports.

- Establishing the hotline telephone numbers (preferably toll-free), which can be a vendor number or a company number that points to the vendor’s number.

- Having local employee liaisons test the hotline website and telephone numbers to ensure the hotline is user-friendly and accessible from each location.

CREATE THE OPERATING FRAMEWORK

**DESIGNATE A HOTLINE ADMINISTRATOR**

Designate a hotline administrator to implement and manage the hotline, including its:

- Access rights.
- Report distribution.
- Reporting analytics.

The hotline administrator should be a high-level employee (such as in-house counsel, a compliance officer, or human resources manager) with:

- A reputation for integrity.
The seniority and training to handle sensitive company information and employee data.

Sufficient authority to take necessary action when the company receives hotline information.

For a discussion on appointing individuals with compliance responsibilities, see Practice Note, Developing a Legal Compliance Program: Build a Team of Compliance Personnel (4-606-5696).

**DRAFT A HOTLINE POLICY**

Draft a hotline policy that encourages employees to speak up when they have legitimate concerns about misconduct. An effective hotline policy should:

- Be simple and easy to understand.
- Communicate the company’s objectives for the hotline and the responsibilities of employees to report misconduct.
- Clearly set out the standards of behavior expected of employees.
- Describe the types of misconduct that should be reported (for example, harassment, fraud, corruption, conflicts of interest, and embezzlement).
- Explain who has access and when, why, and how to use the hotline.
- Offer multiple communication channels for reporting information (in addition to the hotline), such as:
  - an internal reporting chain (such as the employee’s manager, the corporate ombudsman, or the human resources, compliance, or legal departments) for in-person reporting (for a sample internal complaint form, see Standard Document, Discrimination/Harassment/Retaliation Complaint Form (8-501-8053));
  - a dedicated email address;
  - a dedicated fax number; and
  - a dedicated mail address (for example, a P.O. box).
- Outline the procedural steps involved in investigating any concerns and the steps that the company may take if the investigation establishes misconduct (see Best Practices for Employee Discipline Checklist (0-501-7972)).

Emphasize that employees who report concerns in good faith will not be subjected to retaliation and set out the consequences of retaliation (see Prohibit Retaliatory Conduct).

Clarify that employees:

- are not protected from the consequences of their own misconduct by using the hotline (but may be granted immunity or more lenient treatment); and
- face disciplinary action if they provide false or deliberately misleading information.

**PREPARE OPERATING PROCEDURES**

Prepare operating procedures for the hotline that:

- Set a protocol for case management and investigation of hotline reports, including:
  - routing and assigning incidents to appropriate personnel while managing conflicts of interest and segregation of duties;
  - if collective bargaining agreements are in place, properly directing hotline reports that are covered by a grievance process (see Practice Note, Discipline and Discharge Under the National Labor Relations Act: Grievance Procedures (7-523-7065));
  - coordinating investigation-related activities by internal groups such as legal, compliance, human resources, internal audit, and accounting;
  - communicating report contents and investigation status to internal authorities (such as the audit committee or the full board of directors and senior management) and external regulatory bodies, as necessary; and
  - maintaining hotline reports and related records under the company’s record retention policy. For general guidance on retaining and disposing of company records, see Practice Note, Drafting a Document Retention Policy (0-506-7349) and Records Management Toolkit (2-520-1257).

For more information on responding to reports and conducting internal investigations, see Conducting Internal Investigations: Addressing Employee Complaints and Compliance Issues Toolkit (2-502-1874) and Practice Note, Developing a Legal Compliance Program: Seven: Follow-up and Investigations of Complaints and Violations (4-606-5696).

Facilitate the company’s communication with hotline reporters to request additional information and follow up on the progress of the investigation.

Emphasize and maintain the confidentiality of reports (see Practice Note, Handling Employment-Related Internal Investigations: Confidentiality (1-501-9452)).

Include a support strategy for reporters that identifies and addresses risks of reprisal, workplace conflict, or other adverse treatment (see Prohibit Retaliatory Conduct).

Enforce the company’s policy of non-retaliation (see Prohibit Retaliatory Conduct).

Comply with local law (see Understand Local Laws and Culture).

**PROHIBIT RETALIATORY CONDUCT**

Retaliation against employees for reporting misconduct may be a SOX violation, expose the company to liability under state laws for wrongful discharge, and run afoul of local whistleblower protection laws in non-US jurisdictions (such as Canada, China, Japan, and the UK). To minimize the risk of retaliation, the legal, compliance, and human resources departments should take precautionary steps, including the following:

- Discuss with reporters any concerns they may have about retaliatory conduct and ask reporters to flag any potentially retaliatory acts (for example, being reassigned to an undesirable location or being excluded from important meetings).
- Review any performance management (such as decisions concerning compensation, performance reviews, and promotion) or disciplinary action before implementing against a reporter to ensure that the action is not:
  - being taken for retaliatory reasons or timed in a way that creates that impression;
  - less favorable because the employee came forward with concerns; and
  - dissimilar to how other employees in a similar situation are treated.
Meetings with employees (including new hires). Introduce the hotline program and:

- review the company’s policy on compliance and business abuse (see Practice Note, Developing a Legal Compliance Program: Four: Ongoing Training and Communication on Compliance Matters (4-606-5696));
- encourage employee buy-in by explaining how the loss caused by employee misconduct results in the loss of resources and opportunities for everyone at the company;
- assure employees that their good faith reports are protected and can be made without fear of retribution (see Prohibit Retaliatory Conduct);
- explain that hotline reports may be made anonymously (to the extent permitted under local law);
- emphasize that information received through the hotline is kept confidential (to the extent appropriate) (see Practice Note, Handling Employment-Related Internal Investigations: Confidentiality (1-501-9452)); and
- confirm that all reports are considered seriously and acted on appropriately.

Initiatives to create and maintain awareness of and use of the hotline. For example, consider having:

- hotline posters placed in conspicuous, public spaces (such as breakrooms and restrooms);
- hotline wallet cards and brochures distributed to all employees with instructions on how to access the hotline online or via the toll-free telephone numbers listed;
- targeted hotline messages included in regular employee communications (such as newsletters, intranet postings, town halls, and department meetings);
- interactive games and contests offered throughout the year to promote the hotline, with awards and prizes promoting hotline information; and
- periodic reminders of the purpose of the hotline, integrated into the larger corporate awareness programs on compliance and ethics and loss prevention.

Demonstrations of the hotline’s effectiveness. For example, consider:

- following up with employees on the actions taken in response to their reports;
- explaining the positive changes made as the result of hotline reports;
- publicly acknowledging successes, such as assets recovered and attempted misconduct prevented; and
- communicating investigation outcomes in generic or anonymized terms to build confidence that employees are using the hotline and their disclosures are encouraged and dealt with appropriately.

Train managers

The company should train its directors, officers, managers, and supervisors to understand:

- Their role in setting the tone from the top and tone from the middle by modeling ethical behavior and creating an environment that encourages the reporting of concerns (for a discussion of the board’s role, see Article, Board Assessment of Compliance Programs: Reporting (W-006-5910)).
- Hotline operating procedures and use of the hotline.
- The steps to properly address complaints of misconduct and avoid retaliatory actions (see Standard Documents, Whistleblower Reporting: Presentation Materials (W-002-7300) and Responding to Employee Concerns: Supervisor Guidelines (7-501-8765)).
- Company protocols for keeping detailed records of employee performance so that an employee who is disciplined or terminated cannot falsely claim protection under whistleblower
laws. For guidance on effective performance management and recordkeeping, see:

- Practice Note, Conducting Employee Performance Reviews (7-505-9572);
- Best Practices for Employee Discipline Checklist (0-501-7972); and

### TRAIN EMPLOYEES

The company should conduct formal training programs (such as through live training at each employee site and e-learning) for all managers and employees who are given access to the hotline to explain:

- The laws and policies applicable to the company and them (for a collection of business briefings, memoranda, and presentation materials that can be used for training, see In-House Training and Guidance Center (2-564-2345)).
- Who has access and when, why, and how to use the hotline.
- Hotline benefits.
- How to recognize red flags of fraud and bribery as well as unlawful sexual harassment, discrimination, immigration impropriety, or other misconduct. For example, see:
  - Practice Note, The Foreign Corrupt Practices Act: Overview: Recognizing Red Flags (0-502-2006);
  - Foreign Corrupt Practices Act (FCPA) Training for Employees: Presentation Materials (2-586-5086);
  - Complying with US Export Control Regulations Checklist: Perform Due Diligence and Spot Red Flags (1-520-0908);
  - Preventing and Responding to Sexual Harassment Complaints Checklist (4-500-4326);
  - Preventing and Responding to Discrimination Complaints Checklist (5-500-1450); and
  - Drafting an Employment Eligibility Verification Compliance Policy (8-509-5999).

For more information on compliance training, see Practice Note, Developing a Legal Compliance Program: Four: Ongoing Training and Communication on Compliance Matters (4-606-5696).

### ASSESS HOTLINE EFFECTIVENESS

Counsel should partner with the company's internal audit function or engage external resources to regularly audit the hotline program (at least annually) to ensure that:

- It is operating as intended.
- It is effective in preventing and identifying noncompliance or potentially unlawful activity.
- Employees are aware of the hotline.
- Follow-up on hotline reports is timely.
- Feedback and closure are promptly provided to reporters.

The assessment should be conducted as part of the overall compliance program audit and include:

- **Periodic assessments of the hotline vendor’s service level.** For example:
  - make test calls to the hotline to check the quality of the operator service;
  - check the vendor's timeliness in conveying hotline calls and translated hotline reports to the company; and
  - evaluate the quality of those vendor reports.

- **A review of the volume and quality of reports received by the hotline.** For example, heavy hotline usage may indicate significant compliance issues or conversely, that the hotline is working.

- **Interviews and surveys of employees.** The company should understand how employees view the hotline and if they feel comfortable reporting misconduct.

- **An assessment of the steps taken following receipt of a hotline report.** Confirm that hotline policies and procedures are being followed and action taken in a timely manner.

- **Benchmarking of hotline metrics across time or against industry peers.** For example, benchmark the:
  - number and types of reports and inquiries per period;
  - rate of employee use;
  - complaints by location, division, or claim type;
  - percentage of anonymous complaints;
  - time spent per report from report receipt to case closure; and
  - percentage of complaints investigated and substantiated.

- **Continual updates to the hotline program as necessary.** Hotline program updates should take into account the results and recommendations developed from the company's assessment of the hotline.

For more information on compliance audits and hotline assessments, see Practice Note, Developing a Legal Compliance Program: Nine: Monitoring and Auditing of Program Effectiveness (4-606-5696) and Article, Whistleblowing: New risks, new responses: Evaluating hotlines (7-520-4201).

### ABOUT PRACTICAL LAW

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at [legalsolutions.com/practical-law](http://legalsolutions.com/practical-law). For more information or to schedule training, call 1-800-733-2889 or e-mail referenceattorneys@tr.com.