INVESTIGATION · BUSINESS AND CORPORATE INVESTIGATION

# Whistleblowing and the Investigation of Internal Reports

Many serious problems inside organisations come to light because someone reports them. This article explains why people blow the whistle or stay silent, what the law requires, and how internal reports should be received, assessed and investigated so that the organisation learns the truth and the reporter is protected.

ModQu research article · 2,549 words · 23 references (APA 7th edition)

Fraud, safety failures, harassment and corruption are rarely discovered by chance. They are usually reported by someone who saw them: an employee, a contractor, a supplier or a customer. Studies of corporate fraud consistently find that tips are among the most important sources of detection, often more important than audits or regulators (Association of Certified Fraud Examiners, 2024; Dyck et al., 2010). Yet many people who see wrongdoing say nothing, and some who do speak up suffer for it. How an organisation receives and investigates internal reports therefore determines not only whether it learns about particular problems, but whether anyone will tell it about the next one.

This article explains what whistleblowing is, why people report or stay silent, what the law now requires, and how reports should be handled from the moment they are received to the point at which the reporter is told the outcome.

## What whistleblowing is

Near and Miceli (1985) defined whistleblowing as the disclosure by organisation members, former or current, of illegal, immoral or illegitimate practices under the control of their employers, to persons or organisations that may be able to effect action. The definition has three important features. The reporter is an insider, with access to information outsiders lack. The concern is about wrongdoing, not a personal grievance about pay or treatment. And the report is made to someone who can act: a manager, a compliance function, a regulator or, as a last resort, the media.

Whistleblowing can be internal, to people within the organisation, or external, to regulators, law enforcement, legislators or journalists. Most whistleblowers first raise their concern internally and go outside only when they believe they have been ignored or punished (Miceli et al., 2008). This makes the internal response the decisive point. An organisation that handles reports well can investigate and correct problems before they become public scandals; one that handles them badly pushes reporters towards external channels and loses the chance to act first.

## Why people report, and why they stay silent

Research on whistleblowing has examined the characteristics of reporters, the nature of the wrongdoing and the organisational setting. A meta-analysis by Mesmer-Magnus and Viswesvaran (2005) found that intentions to report were related to personal factors such as job performance and role responsibility, and to situational factors such as the seriousness of the wrongdoing and the support of supervisors. Actual reporting was more strongly related to situational factors than to individual ones. In other words, whether people speak up depends a great deal on where they work.

Silence is common. Morrison and Milliken (2000) described organisational silence as a collective pattern in which employees withhold information about problems because they believe speaking up is futile or dangerous. Detert and Edmondson (2011) found that employees hold implicit beliefs about when it is unsafe to speak, such as "don't embarrass the boss in public" or "don't challenge ideas the boss has a stake in", and that these beliefs lead to self-censorship even in organisations that formally encourage voice. Edmondson's (1999) research on psychological safety shows that teams in which people feel safe to raise concerns are better at learning from mistakes.

The fear of retaliation is well founded. Rothschild and Miethe (1999) found that most whistleblowers in their sample experienced some form of retaliation, ranging from ostracism to dismissal, and Alford (2001) documented the long-term harm to the careers, finances and health of many whistleblowers. Kenny (2019) describes how whistleblowers are often positioned as disloyal or unstable, which makes their disclosures easier to dismiss. Any internal reporting system that does not take retaliation seriously will receive few reports.

## The legal framework

Over the past three decades, many countries have introduced legal protection for whistleblowers and duties for organisations to receive reports.

In the United Kingdom, the Public Interest Disclosure Act 1998 protects workers who make qualifying disclosures about wrongdoing from dismissal and detriment. In the United States, the Sarbanes-Oxley Act of 2002 requires the audit committees of listed companies to establish procedures for receiving complaints about accounting and auditing matters, including confidential and anonymous submissions by employees, and protects employees who report securities fraud. The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 created a programme under which the Securities and Exchange Commission pays awards to whistleblowers whose information leads to successful enforcement actions. The regulator reports that the programme has received tens of thousands of tips and paid substantial awards (U.S. Securities and Exchange Commission, 2023).

The European Union's Whistleblower Protection Directive (Directive (EU) 2019/1937, 2019) requires employers with fifty or more workers to establish internal reporting channels. They must acknowledge receipt of a report within seven days, follow it up diligently, and give the reporter feedback within a reasonable period, not exceeding three months. Reporters are protected against a broad range of retaliation, and the burden of proof is reversed: where a reporter suffers a detriment after making a report, it is for the employer to show that the detriment was not caused by the report.

International guidance complements these laws. ISO 37002 sets out guidelines for a whistleblowing management system, built around four principles of trust, impartiality, protection and the handling of reports through a defined process (International Organization for Standardization [ISO], 2021). In the National Health Service in England, an independent review by Francis (2015) found that staff who raised concerns about patient safety were often ignored or mistreated, and recommended a network of "freedom to speak up" guardians to support them.

## Channels for reporting

Organisations usually offer several ways to raise a concern, each with its own strengths and weaknesses.

### Ways to raise a concern

Most organisations offer several channels; each trades off ease of follow-up against protection of the reporter

| | Advantages | Disadvantages |
|---|---|---|
| **Line manager** | Fast; manager knows the context | Manager may be involved or conflicted |
| **Named report to compliance or HR** | Investigator can ask follow-up questions | Reporter may fear being identified |
| **Confidential report** | Identity known only to a few people | Relies on trust that confidentiality will hold |
| **Anonymous hotline or web portal** | Lowers the barrier to reporting | Hard to clarify details or give feedback |
| **External regulator** | Independent; legal protection | Organisation loses the chance to act first |

Based on ISO (2021), Directive (EU) 2019/1937 and Kaplan & Schultz (2007) ModQu.com

Figure 1. Each reporting channel has strengths and weaknesses. Offering several, including at least one that bypasses line management, makes it more likely that concerns will be raised. Diagram by ModQu.

The difference between confidentiality and anonymity is important. A confidential report is one in which the organisation knows who the reporter is but protects that identity. An anonymous report is one in which the organisation does not know. Anonymous channels lower the barrier to reporting: Kaplan and Schultz (2007) found that the availability of an anonymous channel affected intentions to report. But anonymous reports are harder to investigate, because the investigator cannot ask follow-up questions unless the system provides a way to communicate with the reporter without revealing who they are. Many web-based systems now do this.

Stubben and Welch (2020), studying data from a provider of internal reporting systems, found that companies whose employees used the internal system more actively faced fewer and smaller government fines and fewer lawsuits. This suggests that an active internal reporting system is a sign of a healthy organisation rather than a troubled one: problems are being raised and dealt with internally before they grow.

## Handling a report

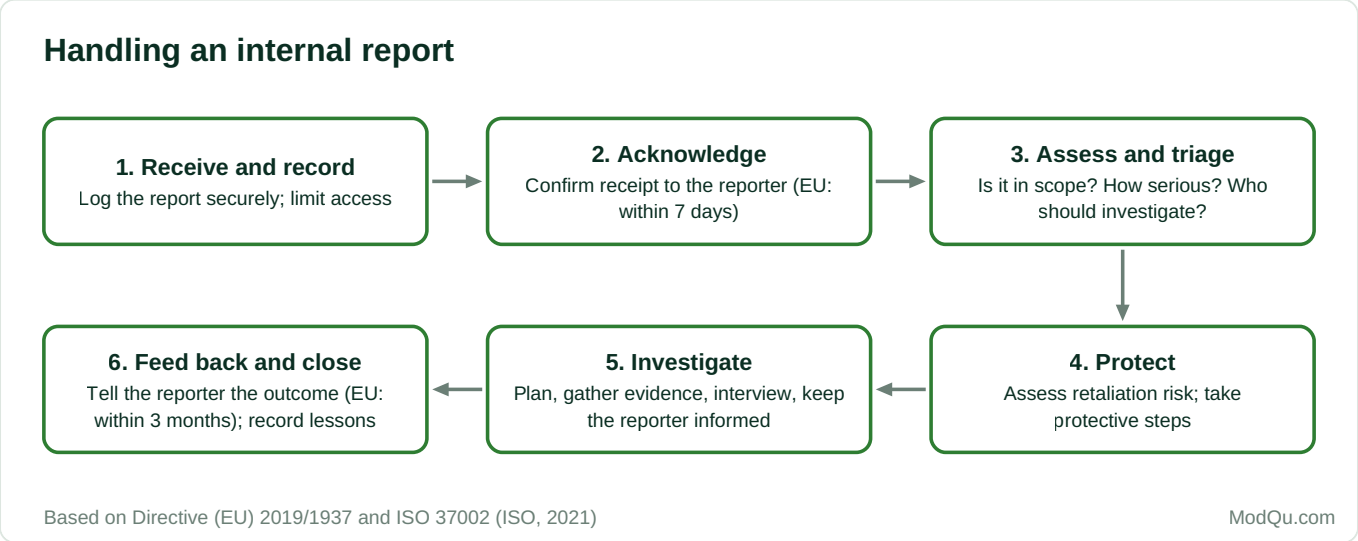



Figure 2. The stages of handling an internal report. Protection of the reporter runs alongside the investigation, not after it. Diagram by ModQu.

### Receive and record

Every report should be recorded in a secure system as soon as it is received, with the date, the channel, the substance of the concern and any documents provided. Access to the record should be limited to the people who need it. A report received orally, for example by a manager, should be written down and, where possible, confirmed with the reporter.

### Acknowledge

The reporter should be told that the report has been received and what will happen next. This simple step reassures reporters that their concern has not disappeared, and under the EU directive it is a legal requirement.

### Assess and triage

Not every report is a whistleblowing matter. Some are personal grievances that belong in a different procedure; some are too vague to act on without more information; some are serious enough to require immediate escalation to the board or to external authorities. Triage decides which route the report should follow, how urgently, and who should investigate. Reports involving senior management should be routed to people who are independent of them, often the audit committee or external investigators. Vandekerckhove and Lewis (2012), reviewing official guidelines, note the importance of procedures that specify clearly who receives and handles reports, and what happens if the normal recipient is implicated.

The assessment should focus on the substance of the report, not the motives of the reporter. Reports made out of personal animosity can still be true, and reports made in good faith can be mistaken. Each is a lead to be tested, not a conclusion to be accepted or dismissed.

### Protect

Protection of the reporter should begin at the triage stage, not after the investigation. The risk that the reporter will be identified, and the risk of retaliation, should be assessed and recorded. Protective steps might include limiting the number of people who know the reporter's identity, designing the investigation so that it does not point back to the reporter, and monitoring for signs of detrimental treatment. ISO 37002 treats protection and support for the reporter, and fair treatment of the people implicated, as integral parts of the process (ISO, 2021).

### Investigate

The investigation itself follows the same principles as any other: a clear statement of what is to be established, impartial investigators, preservation of evidence, fair interviews and a reasoned report. Two features are particular to whistleblowing cases. First, the investigation must be designed to protect the reporter's identity, which may mean gathering documentary evidence before interviews, or interviewing a wider group of people so that the reporter is not singled out. Second, the reporter may be a valuable source of further information, and an investigator who can communicate with the reporter, directly or through an anonymous channel, can ask follow-up questions and test details.

### Feed back and close

Reporters want to know that something was done. They may not be entitled to see the full findings, especially where other people's privacy or legal privilege is involved, but they should be told whether the concern was investigated, whether it was substantiated in general terms, and what action was taken. The EU directive requires feedback within three months. Failure to give feedback is one of the most common reasons reporters lose trust in internal channels and go outside. At closure, the organisation should also record what the case revealed about its controls and culture.

## Fairness to the people implicated

A reporting system must also be fair to the people named in reports. An allegation is not a finding, and the person accused is entitled to know the substance of what is alleged, to see the evidence that matters and to respond before any conclusion is reached. Their identity also deserves protection while the matter is investigated, since a rumour that someone is under investigation can damage a reputation even if the allegation is later found to be groundless. The EU directive requires that the identity of persons concerned be protected for as long as investigations are ongoing, and that they enjoy the right to an effective remedy, a fair hearing and the presumption of innocence (Directive (EU) 2019/1937, 2019).

Fairness to the accused and protection of the reporter can pull in different directions. The accused may need to know what is alleged in enough detail to answer it, and that detail may point to the reporter. Investigators deal with this by relying, wherever possible, on independent evidence such as documents and records, so that the case against the accused does not rest solely on the reporter's word, and by disclosing the substance of the allegation without disclosing its source.

## A short example

The following hypothetical case illustrates the process. An employee in a hospital's procurement team uses the anonymous web portal to report that a manager has been splitting large orders into smaller ones to avoid the threshold above which a competitive tender is required, and that most of the orders go to a company owned by the manager's relative.

The report is logged and acknowledged within two days through the portal's message function. The compliance officer triages it as serious, because it involves possible conflicts of interest and breaches of procurement rules, and passes it to internal audit, which is independent of the procurement department. Through the portal, the investigator asks the reporter for the approximate dates and the names of the suppliers, and the reporter answers.

The auditors extract all orders placed with the named supplier over three years and find clusters of orders just below the tender threshold on the same or consecutive days. Company registry records confirm that the supplier's director shares a surname and address with the manager. Only then is the manager interviewed. The manager is shown the order data and the registry records, and acknowledges the family connection but says it was declared. The declaration register shows no such entry. The investigation finds that the conflict of interest was undisclosed and that orders were split to avoid tendering.

The reporter is told, within the three-month period, that the concern was investigated, that it was substantiated and that action has been taken. Because the case rested on records rather than on testimony, the reporter's identity never had to be revealed. The hospital also changes its purchasing system so that orders to the same supplier within a short period are added together when applying the tender threshold.

## What makes a reporting system work

Research and practice suggest that a reporting system works when employees believe three things: that reporting will lead to action, that they will be protected, and that the process will be fair to everyone involved (Miceli et al., 2008; Brown et al., 2014). Each belief depends on the organisation's track record. Policies and hotlines matter less than what employees see happen to those who use them.

Several practices support these beliefs:

1. **Leadership commitment.** Senior leaders say publicly that they want concerns raised, and act on them.
2. **Multiple channels.** At least one channel bypasses line management, and at least one allows anonymous reporting with two-way communication.
3. **Independence.** Reports involving senior people go to someone independent of them, such as the audit committee.
4. **Prompt, competent investigation.** Reports are triaged and investigated quickly by trained people.
5. **Protection that is monitored.** Retaliation is treated as serious misconduct, and the treatment of reporters is checked after the case closes.
6. **Feedback.** Reporters are told what happened, within a set time.
7. **Learning.** Aggregate data on reports is reviewed by the board for patterns, without identifying reporters.

The volume of reports is not a simple measure of success. A low number of reports may mean that there are few problems, but it more often means that people do not trust the system. A rising number of reports, particularly of named reports, can be a sign that trust is growing. Comparing report volumes with those of similar organisations, and tracking the share of reports that are substantiated, gives a more useful picture.

## The wider view

Culiberg and Mihelič (2017), reviewing several decades of research, note that whistleblowing studies have moved from asking who blows the whistle to asking how organisations respond. That shift reflects a practical lesson. Organisations cannot choose whether wrongdoing will occur, but they can choose whether they hear about it. A reporting system backed by fair, competent and protective investigation is one of the most effective ways of finding out what is really happening inside an organisation, and one of the clearest signals to employees that the truth is wanted.

## References

Alford, C. F. (2001). *Whistleblowers: Broken lives and organizational power*. Cornell University Press.

Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*.

Brown, A. J., Lewis, D., Moberly, R., & Vandekerckhove, W. (Eds.). (2014). *International handbook on whistleblowing research*. Edward Elgar.

Culiberg, B., & Mihelič, K. K. (2017). The evolution of whistleblowing studies: A critical review and research agenda. *Journal of Business Ethics, 146*(4), 787–803. https://doi.org/10.1007/s10551-016-3237-0

Detert, J. R., & Edmondson, A. C. (2011). Implicit voice theories: Taken-for-granted rules of self-censorship at work. *Academy of Management Journal, 54*(3), 461–488. https://doi.org/10.5465/amj.2011.61967925

Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law. (2019). *Official Journal of the European Union, L 305*, 17–56.

Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010).

Dyck, A., Morse, A., & Zingales, L. (2010). Who blows the whistle on corporate fraud? *The Journal of Finance, 65*(6), 2213–2253. https://doi.org/10.1111/j.1540-6261.2010.01614.x

Edmondson, A. (1999). Psychological safety and learning behavior in work teams. *Administrative Science Quarterly, 44*(2), 350–383. https://doi.org/10.2307/2666999

Francis, R. (2015). *Freedom to speak up: An independent review into creating an open and honest reporting culture in the NHS*.

International Organization for Standardization. (2021). *Whistleblowing management systems: Guidelines* (ISO Standard No. 37002:2021).

Kaplan, S. E., & Schultz, J. J. (2007). Intentions to report questionable acts: An examination of the influence of anonymous reporting channel, internal audit quality, and setting. *Journal of Business Ethics, 71*(2), 109–124. https://doi.org/10.1007/s10551-006-0021-6

Kenny, K. (2019). *Whistleblowing: Toward a new theory*. Harvard University Press.

Mesmer-Magnus, J. R., & Viswesvaran, C. (2005). Whistleblowing in organizations: An examination of correlates of whistleblowing intentions, actions, and retaliation. *Journal of Business Ethics*, *62*(3), 277–297. https://doi.org/10.1007/s10551-005-0849-1

Miceli, M. P., Near, J. P., & Dworkin, T. M. (2008). *Whistle-blowing in organizations*. Routledge.

Morrison, E. W., & Milliken, F. J. (2000). Organizational silence: A barrier to change and development in a pluralistic world. *Academy of Management Review, 25*(4), 706–725. https://doi.org/10.5465/amr.2000.3707697

Near, J. P., & Miceli, M. P. (1985). Organizational dissidence: The case of whistle-blowing. *Journal of Business Ethics, 4*(1), 1–16. https://doi.org/10.1007/BF00382668

Public Interest Disclosure Act 1998, c. 23 (UK).

Rothschild, J., & Miethe, T. D. (1999). Whistle-blower disclosures and management retaliation: The battle to control information about organization corruption. *Work and Occupations, 26*(1), 107–128. https://doi.org/10.1177/0730888499026001006

Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745.

Stubben, S. R., & Welch, K. T. (2020). Evidence on the use and efficacy of internal whistleblowing systems. *Journal of Accounting Research*, *58*(2), 473–518. https://doi.org/10.1111/1475-679X.12303

U.S. Securities and Exchange Commission. (2023). *Annual report to Congress: Whistleblower program, fiscal year 2023*.

Vandekerckhove, W., & Lewis, D. (2012). The content of whistleblowing procedures: A critical review of recent official guidelines. *Journal of Business Ethics*, *108*(2), 253–264. https://doi.org/10.1007/s10551-011-1089-1