GLOBAL DISPUTES AND INVESTIGATIONS

RESPONDING TO WHISTLEBLOWERS: A STRUCTURED TRIAGE PROGRAM IS ESSENTIAL

As corporations continue to adopt whistleblower programs, many find themselves struggling to manage burgeoning caseloads. As a result, serious internal fraud investigations can be delayed (with mounting losses) while less consequential complaints are being investigated. The lack of a timely, systematic and repeatable process for evaluating and prioritizing whistleblower tips can also expose an organization to increased regulatory risk.

While there is no single, “right” method for following up on whistleblower complaints, the most effective approaches to handling these cases often resemble the medical triage programs that hospitals and first responders use to allocate limited resources during emergencies. We describe herein some useful guidelines for designing and implementing a fraud triage system.

THE EXPANSION OF CORPORATE WHISTLEBLOWER PROGRAMS

Despite extensive corporate fraud detection measures in place, including closer management scrutiny, and the use of increasingly sophisticated technology, the most common fraud detection method is still the simplest: somebody notices something suspicious and decides to speak up. According to the Association of Certified Fraud Examiners’ (ACFE) 2016 Report to the Nations on Occupational Fraud and Abuse, 39.1 percent of the cases reported in their study were uncovered as the result of anonymous tips (usually from an employee, supplier, or customer).1

The ACFE study also demonstrates that dedicated reporting hotlines are particularly effective. In organizations where such hotlines were in place, 47.3 percent of the cases reported were uncovered through tips, compared with only 28.2 percent of the cases in organizations without hotlines.2 These results are consistent with patterns that have been recorded in the ACFE’s biennial survey since its inception 20 years ago.

On a broader scale, as a matter of best practice, the COSO Internal Control-Integrated Framework, along with various other enterprise risk management (ERM) frameworks and guidance from Institute of Internal Auditors (IIA), also emphasize the importance of establishing and maintaining effective whistleblower programs.

JONATHAN T. MARKS, CPA, CFE
609.219.8867
jonathan.marks@navigant.com

DAVID MANEK
312.583.6841
dmanek@navigant.com

navigant.com

About Navigant

Navigant Consulting, Inc. (NYSE: NCI) is a specialized, global professional services firm that helps clients take control of their future. Navigant’s professionals apply deep industry knowledge, substantive technical expertise, and an enterprising approach to help clients build, manage and/or protect their business interests. With a focus on markets and clients facing transformational change and significant regulatory or legal pressures, the Firm primarily serves clients in the healthcare, energy and financial services industries. Across a range of advisory, consulting, outsourcing, and technology/analytics services, Navigant’s practitioners bring sharp insight that pinpoints opportunities and delivers powerful results. More information about Navigant can be found at navigant.com.
In addition to their demonstrated effectiveness, whistleblower programs have also been promoted through recent regulatory actions. For example, one section of the Dodd-Frank Wall Street Reform and Consumer Protection Act directs the Securities and Exchange Commission to make monetary awards to individuals who voluntarily provide information leading to successful enforcement actions that result in monetary sanctions over $1 million.

A few years earlier, the Sarbanes-Oxley Act of 2002 required the audit committees of publicly traded companies to establish procedures to enable employees to submit confidential, anonymous information regarding fraudulent financial reporting activities.

Dodd-Frank and Sarbanes-Oxley are only two examples out of a broad range of laws that encourage – and often mandate – whistleblower programs. A 2013 study by the Congressional Research Service found no fewer than 40 federal whistleblower and anti-retaliation laws, designed to protect employees who report misconduct. Eleven of those 40 laws were enacted after 1999.

Such laws not only make whistleblower programs more common, they also make the timely resolution of tips even more critical.

RESPONDING TO TIPS – WHY TIMELINESS MATTERS

Dodd-Frank, Sarbanes-Oxley, and the various regulatory structures that were established to implement them are helping to mold a corporate environment where compliance professionals and in-house counsel are incentivized to “blow the whistle.” Programs that offer a reward of other incentives can be helpful in creating a self-regulating environment, but they also make it essential that corporations establish a timely and effective process for remediating complaints.

For example, the SEC established a separate Office of the Whistleblower, which has paid out more than $54 million to whistleblowers since it was founded in 2011. In fiscal year 2015 alone, more than $37 million was paid to reward whistleblowers.

Under this program, if an organization fails to resolve an employee tip within 120 days of it being reported, an audit or compliance professional can report the lapse directly to the SEC and be eligible for a sizable whistleblower award – from 10 percent to 30 percent of any fines or sanctions that are collected.

With incentives like that, it should be no surprise that whistleblower complaints are on the rise. Yet in most cases, such awards would not have been available if the companies involved had resolved the initial fraud complaints within 120 days.

Unfortunately, our experience indicates that, while many companies invest in tips hotlines and similar whistleblower programs, a large portion of them fail to invest adequately in a process for promptly evaluating, prioritizing, and responding to the whistleblowers’ tips in a systematic, repeatable, and defensible manner. As the number of tips grows and investigators’ caseloads expand, complaints end up sitting in a queue waiting to be investigated, while the company remains vulnerable to the risks raised by the tipsters and the SEC timeline for resolving the matters.

For example, a 2016 study by NAVEX Global, a compliance software company, found that the median time to close a case of suspected fraud increased by 18 percent in just the past year, and by 44 percent in the last five years. Moreover, when the various categories of fraud are compared, cases involving suspected accounting, auditing, and financial reporting fraud took the longest to resolve by far – an average of 55 days.

In other words, the average case closure time for cases of suspected financial fraud was almost halfway to the 120-day deadline – the point at which employees are incentivized to report the case directly to the SEC and expose the company to additional, sizable sanctions.

HIDDEN AND DIRECT COSTS OF DELAYED RESPONSE

Even setting aside potential SEC sanctions, delays in investigating whistleblower tips are costly in other ways. Delayed responses to tips can cause employees and other potential sources to lose confidence in the hotline or other whistleblower program, undermining the effectiveness of the program and adding further complexity to the risk management effort.

Most companies expend considerable time, effort, and resources in creating compliance and ethics programs. Failing to establish a system for dealing with allegations or tips in a timely manner can mean those expenditures were wasted.

There are also direct costs associated with delays in handling tips. The losses resulting from a fraud scheme are directly related to how long the scheme occurs. The ACFE’s 2016 Report to the Nations found that the median losses for frauds that were
uncovered in six months or less was $45,000. But at the other end of the scale, schemes lasting more than five years caused a median loss of $850,000. Simply put, the longer perpetrators are able to continue, the more financial harm they are able to cause.

Clearly, the absence of an effective program for handling whistleblower complaints promptly and effectively can have a significant and direct financial impact—in addition to the regulatory, employee relations, and reputational risks such a shortcoming entails.

**A TRIAGE APPROACH**

While there is no single, one-size-fits-all method for following up on whistleblower complaints, the most effective approaches are similar in many ways to medical triage programs, such as those implemented by hospitals and first responders during emergencies to help medical professionals prioritize the treatment of patients.

In medical triage, those with serious, life-threatening injuries are treated ahead of those whose conditions are less severe. In the same way, a fraud triage program helps risk, audit, and fraud professionals prioritize the investigation of tips and whistleblower complaints. Those that indicate serious, material risks are addressed differently and more aggressively than those that reflect mere misunderstandings, minor errors, personal grievances, or false tips, all of which could tie up investigators unnecessarily.

Under a fraud triage program, the same principles apply. Hotline tips or complaints that do not indicate fraudulent behavior can be delegated to human resources, IT, or other line or support functions that are capable of handling them more efficiently. Meanwhile, complaints that involve suspected fraud, but which are less significant in terms of financial losses, control failures or other risks, may be set aside temporarily while larger, more material cases receive immediate attention.

**PROPER STAGING – THE CRITICAL FIRST STEP**

A swift and thorough triage process leads directly to a more appropriate and timely response. The specifics of that response will vary, of course depending on the nature and severity of the case, but the fundamental elements of the treatment include forming the right team to investigate, understand root causes, and provide timely disclosure to all constituencies.

Before such a response can be planned and executed, however, the tip or allegation must be evaluated or “staged” based on a consistent set of criteria. Navigant’s fraud governance framework identifies five such stages:

**Stage 1**

Stage 1 allegations have a low threat level and do not suggest a breakdown of internal controls. Tips that get grouped into this stage do not have a financial or reputational impact. These may include employee-to-employee disputes, isolated cases of small-scale employee theft, and the normal policy complaints, misunderstandings, and personal disagreements that are often raised through a whistleblower program.

In most cases, these complaints are best handled by human resources or management personnel. A basic level of review should be performed and documented to corroborate that no further investigation is warranted. This review and documentation could be performed by a branch or office manager. For an employee who is the target of such a complaint, management should consider placing such employee on a temporary legal hold which triggers the retention of email and other documents until the risk of retaliatory litigation has passed.

**Stage 2**

These allegations are more serious in nature, and often indicate some deficiency in the design of internal controls. Examples include business rule violations such as recurring employee theft or patterns of falsifying expense reports. If the allegation is substantiated, then the result of the remediation process is a change to a business process or business rule, followed by an enhancement of the company’s preventive or detective internal controls.

Because they indicate a deficiency in internal controls, such allegations are escalated to the internal audit function in order to obtain a deeper understanding of the control environment. Internal audit should evaluate what controls are currently in place, and determine where the breakdown in internal controls occurred.

It is also important to assess if the allegations are signs of a bigger problem or if they could have an impact on financial reporting. If financial reporting is affected, sensitivity testing must be performed to calculate the low case, medium case, and worst case financial impact.
Internal audit’s review also might identify multiple violations. Again, the employees affected should be put into a legal hold which triggers the retention of email and other documents until the risk of litigation passes. In some cases, employee termination may be warranted.

**Stage 3**

These allegations generally involve an override of internal controls, and thus are at a minimum a serious deficiency. But they have only a minimal impact on the financial statements or the company’s reputation. More serious allegations in this category include fraud, embezzlement, and bribery and corruption involving employees, mid-level management or third-party vendors.

Such cases require the same level of investigation as Stage 2 cases, along with an internal investigation that usually is conducted under the direction of the general counsel, involving compliance and internal audit as well. In some instances, the investigation might need to be performed independently by a function or person who is not directly involved in the control environment.

**Stage 4**

These are serious allegations that could have an impact on the completeness and accuracy of the audited financial statements, and that could indicate a material weakness in internal controls. They do not, however, appear to involve any member of the senior management team.

Such cases are generally addressed through an internal investigation, usually under the direction of outside counsel operating under privilege. The investigation often involves the use of independent, outside experts as well.

**Stage 5**

 Allegations in this category involve one or more members of the senior management team, or are serious enough to damage the company’s reputation. The receipt of allegations in this stage usually place the company into crisis management mode, and could result in the restatement of audited financial statements or added regulatory scrutiny.

In such instances, the board generally should engage outside counsel and forensic investigation experts to initiate a privileged and confidential fact-based investigation. The external auditors may also be involved and a disclosure to the SEC may be required.

It’s important to note that, in both Stage 4 and Stage 5, engaging outside experts is generally necessary. Other critical elements of the Stage 4 and Stage 5 responses include having a qualified and experienced investigation team, along with a time-phased work plan that minimizes disruptions to the organization’s day-to-day business as much as possible.

The investigators will begin with fact-finding interviews to help them evaluate who else to interview and when. The investigators will also help the company identify a list of custodians who will be interviewed to understand where their data was being saved (e.g., on email servers, mobile phones or other devices, flash drives, cloud servers, and network folders).

Generally, a large-scale data collection effort will then ensue in order to search and preserve all potentially relevant information. The goal is to determine who knew what and when, and how high up the chain the knowledge went.

The investigation will also assess the audited financial statements, so that counsel and board members can determine what disclosure requirements might apply. In addition, where internal control issues are noted, outside counsel can also recommend and assist in recommending new or enhanced policies, procedures, and controls.

**OWNERSHIP, RESPONSIBILITY AND FOLLOW-UP**

Obviously, the triage staging system described here is not the only plausible methodology an organization can use for evaluating allegations of wrongdoing and planning appropriate responses. Other thought leaders in the field have proposed evaluating tips according to various other criteria such as the severity of the allegation, the specificity of the information it contains, and similar factors.7

Ultimately, whatever triage or prioritization approach is chosen it will need to be customized to reflect the company’s particular situation and industry. In many instances, boards may choose to combine elements from several approaches.
Regardless of the specific criteria upon which the system is based, the importance of maintaining written policies and procedures cannot be overstated. Moreover, it is important in all cases that the responsibility for developing, implementing, and maintaining the response system be clearly defined.

The assignment of this responsibility will vary as well, depending on the size and nature of the organization, its governance structure, the volume of whistleblower complaints and other factors. It could fall to internal audit, the corporate general counsel, a board committee, a designee of the CFO, or some other person or group – but in all cases it’s essential to have a designated individual or business function that is responsible for initially capturing complaints and performing the triage.

Once the framework is set and data is being collected, it’s also important to step back and periodically assess what the data is saying. For example, if the complaint hotline is bombarded with a high frequency of inconsequential complaints related to minor personnel disputes or employees complaining about having to work a holiday, then it may be time to provide additional training on how the complaint hotline is to be used.

On the other hand, an increase in sexual harassment complaints or complaints related to substandard working conditions could provide early warning of a potential class action lawsuit. Similarly, an increasing number reports of low dollar employee theft are usually signs of a larger cultural problem.

Evaluating the data and trends captured in your complaint system can help you make decisions that could prevent the next “big event.” In that sense, an effective, well-designed, and consistently executed fraud triage effort can pay even bigger dividends that go beyond the direct benefit of helping you evaluate and prioritize tips and complaints more efficiently.

David Manek is a director and national leader of Navigant’s Technology Solutions Structured Data Practice. His expertise is focused in the area of helping clients through event-driven crises by leveraging a deep bench of experts and leading technology to solve problems.

Jonathan T. Marks, CPA, CFE, is a managing director with Navigant in their global disputes and investigations practice. He works with outside counsel, boards of directors, audit committees, and officers in conducting forensic accounting investigations, assisting companies in developing remedial procedures and designing governance, risk management, and compliance systems and internal controls to mitigate future potential issues.

2. ibid., page 27
6. Report to the Nations, page 17
7. See, for example, Financial Statement Fraud: Prevention and Detection, by Zabihollah Rezaee and Richard Riley, which recommends a system of four protocols for handling various types of tips. (Rezaee, Zabihollah; Riley, Richard, Financial Statement Fraud: Prevention and Detection, John Wiley & Sons, September 2009)