Responding to Investigations: Considerations for General Counsels & Compliance Officers

Rachel B. Goldman, Bracewell LLP
Thomas F. Kokalas, Bracewell LLP

Introductions

Overview

I. Compliance personnel are frequently called upon by companies to respond to, address and remediate sensitive and complex investigations.

II. The presentation will outline the keys to successfully handling internal and regulatory enforcement matters and highlight pitfalls and risks that often arise during these investigations.

III. In addition, we will outline specific steps General Counsels and Compliance Officers should consider during “blue sky” days to ensure their departments are adequately prepared for substantive inquiries.
Hypothetical Case Study

- During a routine meeting with Internal Audit to conduct a final review of earnings just prior to the release of very strong quarterly financial results, a career mid-level Controller identifies a series of journal entries in an internal account that cannot be properly reconciled or explained.
- The numbers were labeled “pre-paid expenses,” which had the effect of increasing earnings and profits, while reducing overall expenditures. The total expense items have now grown to a “material” amount because the entries have been made in every quarter over the last three years.
- A quick records search shows that the expenses were entered by Operations and were tied to goods and services specifically for the gas business.
- Four years ago, after a series of Grade 2 and a few Grade 1 leaks, the Commission entered an Order that required the company to upgrade its gas lines and equipment – expenses that were deemed not recoverable in future rate cases.

Hypothetical Case Study (Cont’d.)

- Multiple emails and attempts by the mid-level Controller to speak with the Head of Operations and the Chief Financial Officer about the “expenses” over the last three weeks have gone completely unanswered.
- It has also been discovered that Procurement has almost no purchasing records related to the relevant gas equipment.

3:20 PM on a Friday Afternoon:

- Internal Audit sends you this information via email with specific facts in a 7 page, single spaced memorandum.
- That same afternoon, the General Counsel forwards you a subpoena from the local US Attorney’s Office requesting accounting information and emails for all employees in the gas business for the last 10 years.
- Also, the Commission just called Operations to schedule a Compliance Audit related to the 4 year old Order.

Responding to Investigations:
Responding to Investigations (Cont’d.)

What steps should you take to respond?

- Preserving Documents?
- Reviewing Documents and Conducting Interviews?
- Written Report of Findings?
- How can we maintain the integrity of the investigation?
- Is the CFO involved?
- Head of Operations?
- Communicating with the Regulators and Responding to Multiple RFIs?
- Does the CEO know?
- Should we inform the Board?
- The Audit Committee?
- Retain Outside Counsel?

Investigation Timeline

SECTION 1 Response Team

Initial Considerations

Collect and Review 3P Vendors

Investigation and Findings

Exhibit and Review

New Data

Deferred Prosecution

Cooperation

Compliance and Commitments

Remediation Efforts

Establish the Facts

SECTION 2 Interviews

Document Production

Meetings with Regulators

Remediation Efforts

Establish the Facts

SECTION 3 Remediation Efforts
Responding to Investigations (Cont’d.)

Initial Considerations:
- Partner with General Counsel and Create a Response Team
  - Create Reporting Group
- Ensure all Constituents are Apprised of Response Plan
  - Board
  - Audit Committee
  - Management
- Engagement with Outside Counsel
  - Privilege Considerations
  - Independent Evaluation
  - Managing Discussions with Regulators
- Engagement with Third Party Vendors
  - Document Preservation, Collection and Review
  - Accounting and Financial Analyses
Investigation Timeline

Responding to Investigations (Cont’d.)

Document Preservation and Collection
- Conduct Initial Interview(s)
- Ascertain the Departments Involved
- Identify Employees with Relevant Information
- Content Specific
- Distributed to All Relevant Employees
- Receipt Confirmations
- Engage the IT Department Immediately
- Prevent Deletion and Spoliation
- Extract Information to Store on Review Platform

Responding to Investigations (Cont’d.)

Conducting the Factual Interviews
- Assignment of Personnel to Conduct Task is Critical
- Notes and Memoranda / Privilege
- Corroborating the Information with Documentary Evidence
- Conducting Multiple Interviews of the Same Individuals

The Document Review
- Piecing the Information Together
- Creating a Chronology of Events

Responding to Regulators
- Negotiating Document Requests
- Meet Early and Often, But Not Too Much
- Mitigation and Negotiating the Settlement

Findings and Conclusions
- Report of Findings and Remediation
- Assess Violations
Responding to Investigations (Cont’d.)

The Remediation Plan

- Development of Remediation Plan Occurs Concurrently with the Investigation
- Work with a “Clean Team” from the Business Side
- Remediation Plan Approved by Board or Audit Committee
- Public Relations
- Cost Concerns

Hypothetical Case Study Remediation:
- Restatement of Historical Financials
- Review of Gas Installations
- Upgrade Where Necessary
- Address any Public Safety and Trust Concerns
“Blue Sky” Protocols

Important Tools and Considerations
- Create pre-approved document preservation notices
- Ensure the IT department has the ability to seamlessly preserve and extract data from various sources, including cloud based storage, mobile devices and emails.
- Pre-identify vendors the company will use to lock in contracts and pricing.
- Identify protocols for retaining outside counsel.
- Ensure public relations team is prepared for rapid response to inquiries and pro-active communications strategies.
- Periodic Risk Assessments.

“Blue Sky” Protocols (Cont’d.)

Compliance Dashboards

<table>
<thead>
<tr>
<th>Compliance Risk Area</th>
<th>Risk level</th>
<th>Principal risk</th>
<th>Trend or Prior year</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber security</td>
<td>High</td>
<td>Cyber security Risk 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>Medium</td>
<td>Privacy Risk 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FERC</td>
<td>Medium</td>
<td>FERC Risk 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental</td>
<td>Low</td>
<td>Environmental Risk 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>State Regulatory</td>
<td>Low</td>
<td>State Regulatory Risk 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Conclusion

QUESTIONS AND ANSWERS