



Internal Investigations, Confidentiality and Witness Statements

HR Best Practices Webinar Series

June 5, 2013

Presented by:

Daniel B. Pasternak	Partner	Phoenix, Arizona
Kerryn L. Holman	Associate	Phoenix, Arizona



What Is a Workplace Investigation?

- Tool to learn about, respond to, and, if appropriate, discipline employees for suspected:
 - Misuse of company time/leave/benefits
 - Discrimination, harassment, or retaliation
 - Theft, destruction, or vandalism of property
 - Misappropriation or misuse of confidential information or trade secrets
 - Substance abuse
 - Workplace violence
 - Unfair business practices toward consumers
 - Employee negligence
 - Quality assurance failures
 - Health and safety violations, security, weapons in the workplace
 - Other violations of company policy

Why Conduct a Workplace Investigation?

- Determine whether policies or procedures have been violated
- Assure adherence to company goals, mission, and values
- Facilitate appropriate employee discipline
- Assure quality in products, services
- Ensure a sound, factual basis for informed decision-making
- Reduce exposure to claims (risk management)

Why Conduct a Workplace Investigation?

- Comprehensive and compliant investigations further the company's goals by ensuring:
 - Reliable documentation exists for future decision-making and/or litigation
 - Percipient witnesses are identified and credibility assessed
 - Evidence is preserved
 - Key legal defenses are maintained, e.g., *Faragher/Elterth* defense to harassment claims, *Kolstad* defense to punitive damages (good-faith efforts to comply, even where malicious/reckless indifference)
 - Employees understand the company's commitment to objective, fair treatment of employees

What Events Might Trigger a Need to Conduct a Workplace Investigation?

- Complaint or report of violation
 - Even if complainant or victim insists on no action
- Accusation
- Management observation
- “Reason to know or suspect” misconduct
- Injury or illness
- Suspected substance abuse
- Threats
- Vandalism, sabotage, theft
- Violation of work rules
- EEOC, ACRD, NLRB, or other charge
 - Even if employee did not complain internally
- DOL audit

What Laws Might REQUIRE a Workplace Investigation?

- Discrimination laws (Title VII, ADA, ADEA, etc.)
 - *Farragher/Elterth* defense
- OSHA
- Drug Free Workplace Act (federal contractors)
- SOX
- Securities Acts
- DOT regulations
- HIPAA

What Type of Workplace Investigation?

- “Formal” Investigation
 - Possible legal exposure
 - Serious violation of policy
 - i.e., EEO policies, drug/alcohol policy, HIPAA violation
 - Documentation of investigation and result is needed

- “Informal” Investigation
 - Minor policy violations
 - i.e., workplace conflict
 - Quickly resolved misunderstanding

Is a Formal Investigation Required?

- Consider...
 - One incident or pattern of conduct?
 - Are all facts known?
 - i.e., one offensive email, voicemail, or other communication, identity of sender not disputed, or conduct directly observed?
 - How serious is the alleged conduct?
 - How many employees are involved?
 - Is medical, financial, or trade secret information involved?
 - Who is the complainant/accused?

Is a Formal Investigation Required?

- What internal policy or area of law is implicated?
 - Securities, financial practices, SOX, FCPA
 - Business practices towards customers, advertising
 - Consumer fraud; FTC
 - Employment laws
 - Title VII, FLSA, etc.
 - Relationships with vendors/suppliers
 - Safety/security/weapons/workplace violence
 - Workplace-related employee complaints

When Should a Workplace Investigation Take Place?

- ASAP!!! Why?
 - Memories fade, emotions (and stories) change
 - Documents (especially electronic communications) get lost or destroyed
 - Witnesses may quit or be fired
 - Prevent witnesses from “getting their stories straight”
 - Prevent spoliation, adverse inference instruction
 - Legal duty to investigate promptly
 - *Faragher/Ellerth* defense, Dodd-Frank, OSHA

What Makes Up a Good Workplace Investigation?

- Prompt, but well-planned
- As thorough as necessary, but does not “drag on”
- Impartial, objective, critical
- As confidential as is reasonable
- Detailed, well-documented
- Appropriately tailored to objectives
- De-escalates emotions and tension in the workplace
- Conducted by disinterested and respected persons
- Recognizes employee privacy concerns
- “Spin-free zone”
- Meaningful outcomes for interested persons
- Effective at facilitating an appropriate outcome
- Closure – fix and move on
- Truthful – ER 4.1

Workplace Investigation: Process Overview

1. Identify goals and plan
2. Pick an investigator or investigative team
3. Gather documents
 - a. Personnel files of complainant and accused
 - b. Prior complaints
 - c. Medical files if appropriate (HIPAA)
 - d. Correspondence, e-mails, other documents
 - e. Notes
 - f. Relevant workplace policies
 - g. CBA
4. Investigator File
 - a. Interview notes from all investigators
 - b. Written plan/list of interviews
 - c. Signed statements
 - d. Final report (with conclusions and recommendations, as appropriate)
5. Consider Additional Resources
 - a. PR or crisis consultants
 - b. Outside counsel
 - c. Private investigators and/or surveillance outside of work (i.e., work comp fraud)
 - d. IT needs
 - e. Law enforcement

Who Should Conduct a Workplace Investigation?

- Human Resources
 - Particularly for general violations of company policy
- Manager/Supervisor
 - Fact gathering only
- Outside consultant/investigator
 - Particularly if a conflict of interest - **ER 3.7**
- In-house or outside counsel
 - Particularly if a threat of litigation or criminal consequences
- Forensic examiners
 - Particularly if electronic data at issue
- Law Enforcement
 - If theft, violence, or illegal drug use is suspected

Who Should Conduct a Workplace Investigation?

- Traits:
 - Credible, respected, impartial, knowledgeable about company policies and employment law issues, good interviewing skills, well-organized, trustworthy, no conflict of interest
- Should not:
 - Prejudge the complainant, accused, or the outcome
 - Be friends (social media or otherwise) with subjects of the investigation
 - Make subjective determinations (i.e., credibility of witnesses) without first conducting a complete and objective investigation
 - Be put in an awkward position (i.e., investigating a superior; fear retaliation for a quality investigation; simultaneously be a witness and an investigator)

Who To Interview?

- Decide who to interview
 - Complainant
 - Victim (if not complainant)
 - Accused
 - Witnesses
 - Employees in same department/work area
 - Employees the complainant/victim/accused/management identify
 - Authors of relevant documents
 - Management
 - HR
 - Executives/Board members
 - Experts within the company (e.g., trained equipment operator in an injury incident involving the equipment)
 - Others outside the company?
- In what order?
 - Typically: complainant/victim→accused→witnesses→complainant/victim

Where to Conduct Interviews

- Key is to make the interviewee secure and willing to open up
 - avoid negative perceptions and influences:
 - Private room
 - Interviewee's office
 - Off-site
 - No time limits
 - Avoid false imprisonment
- Consider safety of interviewer

Interview Techniques

- Prepare an opening statement
 - Thank interviewee
 - Explain what you are investigating
 - Explain why interviewee was selected
 - Company takes matter seriously, has a commitment to investigate the claim
 - Cooperation is expected
 - Company has firm no-retaliation policy
 - Information will be kept “as confidential as possible” or will be disclosed on “need to know” basis

Interview Techniques

- Use traditional, “deposition-style” techniques (with a caveat)
 - Ask open-ended questions
 - Don’t dominate the conversation
 - Allow plenty of time for responses; don’t rush
 - Active listening and follow-up
 - Cover all bases (“is there anything else you can think of?”)
- But, it’s not a deposition...
 - ER 4.3, 1.13(f)
 - ER 4.4

Interview Documentation

- Written statement from witness
- Recorded interview/statement from witness
 - Consent issues are state-specific
- Court reporter transcript (rarely)
- Interview notes
- Memorandum summary
- Relevant documents for each interview
- Written notes
 - During interviews
 - After interviews
 - Personal observations vs. reported facts
- Report
 - Comprehensive final product
 - Include recommendations for action?

Other Potential Sources to Investigate?

- Emails
- Text messages
- Instant messages
- Voicemails/telephone records
- Home computers
- Personal electronic devices
- Documents (electronic and hard-copy)
- Video/audio surveillance
- Social networks

BUT...beware of NLRA surveillance issues and privacy issues...

Format of Final Report

- Consider final format of report
 - Formal, detailed report; summary of findings; or memo to file?
- Consider who will see the investigation and its results
 - Board of Directors
 - Outside auditors
 - Inside/Outside counsel
 - Government agencies
 - Plaintiff's attorneys
 - Press
 - Law enforcement

The Outcome

- Appropriate punishment
 - Adequate for the misconduct
 - Consistent with past practices
 - Sufficient to avoid future problems (e.g., transfer away from complainant)
 - Deterrent effect
- Appropriate remedy to the victim
 - Restore any lost job benefits
 - Report results of investigation, as appropriate
 - Confirm in writing, as appropriate
- Consider education to prevent future occurrences

What Not to Do...

- Defame
- Polygraph
 - Employee Polygraph Protection Act
- Use leading questions
 - i.e., “Did you grab her arm or did you just happen to bump into her?”
- Assume/jump to conclusions
- Fail to act
- Fail to train
- Violate ADA, HIPAA, FCRA, privacy rights

What Not to Do...

- Most important – no retaliation
 - “[T]hose ... employer actions that would have been materially adverse to a reasonable employee or job applicant” or that “could well dissuade a reasonable worker from making or supporting a charge of discrimination.” *Burlington Northern v. White*, U.S. Supreme Court (2006).
- Everyone involved in the investigation process is protected to a certain degree
 - Complainant, victim, accused, witness, investigator
- Ensure all employees understand that retaliation will not be tolerated
- Particularly important in cases involving alleged whistleblowing activity
 - SOX; Dodd-Frank; False Claims Act

Special Issues to Consider...

- Attorney-Client Privilege
 - *Upjohn v. United States*, 449 U.S. 383 (1981)
 - Communications between company counsel and company employees are privileged if the communications occurred to assist counsel in providing legal advice to company.
 - » See **ER 1.13, Comment 2**
 - But, must give a corporate “Upjohn” warning (like a Miranda warning)
 - Counsel represents the company, not the individual
 - » See **ER 1.13(f); 4.3**
 - Employee being interviewed to assist counsel in providing legal advice to company
 - Statements made by employee will be shared with company
 - Communications are privileged
 - Company alone owns the privilege
 - In house counsel (and others) should begin with an *Upjohn*-type warning
 - Encourage truthfulness
 - Discuss one-way confidentiality

Special Issues to Consider...

- Rights of the Interviewee
 - Right to counsel?
 - If accused is facing possible criminal charges
 - If employee reasonably believes answer would incriminate them in a criminal case
 - Right to a “friend?” (*Weingarten* rights)
 - Right to union representative?
 - Consider whether CBA applies to investigations of complaints
 - Can an employee refuse to participate? Advise of consequences of refusal?

Special Issues to Consider...

- Confidentiality Issues
 - Can employer impose a blanket rule obligating employees to keep ongoing workplace investigations confidential?
 - NLRB's position (*Banner Health System*, 358 NLRB No. 93 (2012); NLRB Advice Memorandum (January 29, 2013)):
 - Employer cannot maintain a blanket policy/rule regarding the confidentiality of employee investigations.
 - » Section 7 of NLRA – employees have right to discuss discipline or disciplinary investigations involving fellow employees.
 - Employer must demonstrate a need for confidentiality on a “case-by-case basis” – is there a “legitimate and substantial business justification” that outweighs Section 7 rights?
 - » Witnesses need protection?
 - » Evidence in danger of being destroyed?
 - » Testimony in danger of being fabricated?
 - » Need to prevent a cover-up?
 - EEOC has taken a similar position
 - Issued a predetermination letter suggesting blanket rule on confidentiality violates Title VII

Special Issues to Consider...

- Confidentiality Issues

- NLRB's example of a lawful rule/policy statement on confidentiality of investigations:

"[Employer] has a compelling interest in protecting the integrity of its investigations. In every investigation, [Employer] has a strong desire to protect witnesses from harassment, intimidation and retaliation, to keep evidence from being destroyed, to ensure that testimony is not fabricated, and to prevent a cover-up. [Employer] may decide in some circumstances that in order to achieve these objectives, we must maintain the investigation and our role in it in strict confidence. If [Employer] reasonably imposes such a requirement and we do not maintain such confidentiality, we may be subject to disciplinary action up to and including immediate termination."

- NLRB Advice Memorandum (January 29, 2013), p. 1 & fn. 7.

Special Issues to Consider...

- Be aware of privacy issues
 - General issue: does the employee have a reasonable expectation of privacy?
 - California – constitutional right to privacy
 - *City of Ontario v. Quon* (SCOTUS)
 - *4th Amendment issue: Court assumed public employee had a reasonable expectation of privacy in text messages, but held that the City's search was reasonable*
 - *"Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that defined the existence, and extent of privacy expectations enjoyed by employees when using employer-provided communication devices."*

Special Issues to Consider...

- Be aware of privacy issues
 - *Loving Care Agency, Inc. v. Stengart (NJ)*
 - *Employee used company computer to send correspondence to her private attorney using password-protected Yahoo! email account*
 - *Issue: did the employee waive confidentiality of her emails because she sent and received them via a company-provided laptop?*
 - *Outcome: despite the employer's written policy explaining that email communications are not considered private, the court concluded that the employee had a reasonable expectation of privacy, and thus the privilege was not lost.*
 - *Why?*

Special Issues to Consider...

- Be aware of privacy issues
 - Friends of *Stengart*
 - *Haynes v. Office of Att’y Gen. Phill Kline*: reasonable expectation of privacy in private files stored on office computer.
 - *Pure Power Boot Camp v. Warrior Fitness Boot Camp*: reasonable expectation of privacy in web-based emails accessed on office computer.
 - *United States v. Long*: reasonable expectation of privacy in emails sent through employer’s email system on office computer.
 - *Schill v. Wisconsin Rapids School District*: private emails sent from a government account are not public records under state’s sunshine law.

Special Issues to Consider...

- Be aware of privacy issues
 - Foes of *Stengart*
 - *McLaren v. Microsoft Corp.*: no reasonable expectation of privacy in private files stored on office computer.
 - *Smyth v. Pillsburg Co.*: no reasonable expectation of privacy in emails sent to company supervisor.
 - *TBG Ins. Serv. Co. v. The Superior Court of Los Angeles County*: no reasonable expectation of privacy in content stored on employer-provided home computer.
 - *United States v. Angevine*: no reasonable expectation of privacy in content stored on office computer.

Special Issues to Consider...

- Be aware of privacy issues – social networking
 - Recent congressional bills awaiting approval (Social Networking Online Protection Act; Password Protection Act of 2013):
 - Would prohibit employers from demanding direct access to current and prospective employees' password-protected social networking accounts, personal email accounts, and other “personal user generated content.”
 - No demands for employees' or applicants' passwords.
 - No demands for employees or applicants to log into their accounts so that employer can browse.
 - No demands for employees or applicants to “friend” the employer as a term of new or continued employment.

Special Issues to Consider...

- Be aware of privacy issues – social networking
 - Some form of social networking privacy legislation has been enacted or is pending in at least 36 states.
 - Some form of legislation has been enacted in (among other states):
 - Arkansas
 - California
 - Colorado
 - Delaware
 - Illinois
 - Maryland
 - Michigan
 - New Mexico
 - Oregon
 - Utah
 - Vermont
 - Washington
 - Some form of legislation is pending in Arizona (S.B. 1411) and Ohio (S.B. 45), among other states
 - Implications for internal investigations?
 - Can't require subjects of an internal investigation to grant access to their online social networking accounts or other personal user-generated content as part of investigation or otherwise.

Strategies for Avoiding Claims

- Regularly train managers and supervisors on policies
- Develop and disseminate policies to lower privacy expectations, especially in electronic communications (right to monitor)
- Investigate only based on reliable, documented factual allegations that justify investigation
- Do not investigate more than necessary
- Maintain confidentiality to the extent possible
- Utilize the appropriate investigator
- Make decisions and take action

Summary

- Identify the type of complaint and the policies or laws it implicates
- Evaluate how best to conduct the investigation
 - Formal or informal investigation
 - Who is the right person to investigate
 - Who needs to be notified right away (i.e., IT)
- Plan the investigation
 - Gather documents and information
 - Identify witnesses
 - Determine what type of final product will be required

Summary

- Conduct interviews and gather facts
- Prepare an objective, written report (if appropriate)
 - Consider whether the report should contain conclusions or recommendations
- Report the findings of the investigation to the appropriate people
- Take action, if appropriate (i.e., discipline)
- Report findings and remedial action taken, if appropriate, to complainant, and to any required government agencies
- Secure and preserve the investigative file

Questions?

Credit Information

- For those you who require CLE/CPD or HRCI credits please note the following states have been approved, California, Florida, Ohio and Texas; as well as Arizona, New York, and New Jersey through state reciprocity laws. CPD and CPE have also been approved. If you require credit in a jurisdiction not pre-approved we can assist.
- Tomorrow you will receive an email with a link to an online affidavit. Open this link and complete the form. Don't forget to include the affirmation code on the form. Once completed, PDF a copy of the signed form to Robin Hallagan at robin.hallagan@squiresanders.com
- Remember to complete the webinar survey immediately following the end of this presentation. You are required to complete this evaluation before receiving a certificate of attendance.