Today's Investigation, Tomorrow's Risk:

"*How to avoid pitfalls in doing investigations"*

RIM's 2013 E-Day

Understanding the risk's we are trying to avoid in doing investigations: Civil Liability, Criminal Liability, and Reputation Liability

Legal Review: Laws that can/may trigger litigation over employee investigations:

Privacy of Communications
The Electronic Communications Privacy Act (1986)
Telephone Consumer Protection Act of 1991

Children's Privacy
Children's Online Privacy Protection Act (COPPA) of 1998

Privacy of Financial Information
Fair Credit Reporting Act (1970)
Right to Financial Privacy Act (1978)
Taxpayer Browsing Protection Act (1997)
Gramm-Leach-Bliley Act (1999)
Fair and Accurate Credit Transactions Act (2003)

Privacy of Government Collections
Census Confidentiality Statute of 1954
Freedom of Information Act (1966)
Privacy Act of 1974
Computer Security Act of 1987
E-government Act of 2002

Privacy of Medical Records
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
**Note: In December of 2003, the Fair and Accurate Credit Transactions Act limited the sharing of medical information in the credit industry*.

Privacy of Miscellaneous Records and Activities:
Administrative Procedure Act (1946)
Family Education Rights and Privacy Act (1974)
Census Confidentiality Statute (1954)
Administrative Procedure Act (1966)
Freedom of Information Act (1966)
Fair Credit Reporting Act (1970) *Modified in 2003 FACTA
Privacy Act of 1974
Family Education Rights and Privacy Act (1974) *also known as the Buckley Amendment
**Note: The Patriot Act of 2001 narrowed the CCPA privacy provisions, clarifying that companies who offer cable-based Internet or telephone service will be subject to the requirements of the Cable Act to notify subscribers of government surveillance requests only when detailed cable viewing information is being sought. Otherwise, cable operators can respond to a government surveillance request under ECPA, which does not require service providers to notify subscribers of requests.*

The Electronic Communications Privacy Act (1986) * also known as the ECPA
Computer Security Act (1987)
Employee Polygraph Protection Act (1988)
Video Privacy Protection Act of 1988
Telephone Consumer Protection Act of 1991 * also known as the TCPA
Driver's Privacy Protection Act of 1994
Communications Assistance for Law Enforcement Act of 1994 *also known as CALEA
Telecommunications Act (1996) Customer Proprietary Network Information (CPNI)
Taxpayer Browsing Protection Act of 1997
Gramm-Leach-Bliley Act (1999)
Wireless Communication and Public Safety Act (1999)
E-Government Act (2002)
Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003
Fair and Accurate Credit Transactions Act of 2003 * also known as FACTA
Do-Not-Call Implementation Act of 2003

Legal Review Continued: Discussion

Employers increasingly are being challenged in court for their use of criminal background checks, according to a March 23, 2011, report by the National Employment Law project. The National Employment Law Project report asserted that "after years of dormancy, the basic civil rights and consumer protection laws restricting the use of criminal records are catching a second wind." At least five major civil rights lawsuits against large employers were filed in 2010 challenging the use of criminal background checks, the report noted. The report noted that the U.S. Equal Employment Opportunity Commission (EEOC) has stated that "an absolute bar to employment based on the mere fact that an individual has a conviction record is unlawful under Title VII." Yet it also observed that Title VII does not wholly bar the use of criminal records in employment decisions.

Cases:

In Arroyo v. Accenture, Accenture has been challenged for rejecting job applicants and terminating employees with criminal records, even where the criminal history has no bearing on the fitness or ability to perform the job, according to the report.

In Hudson v. First Transit Inc., First Transit has been challenged for allegedly having a blanket policy prohibiting individuals from working for the company if they have been convicted of a felony or served a day in jail.

In Mays v. Burlington Northern Santa Fe Railroad Co. (BNSF), BNSF was sued for allegedly having a blanket policy prohibiting any person with a felony conviction in the previous seven years from being employed at its facilities.

In the class-action lawsuit Johnson v. Locke, the U.S. Census Bureau was sued under Title VII for discriminating against people with criminal records by excluding them from consideration for temporary positions with the Census.

Backgrounds checks in discussion: *Employers need to be careful about using once single source for background checks and then making decisions based on that single source of information. There is no single trusted source of information for background checks and the information brokers on a whole do not really care at the end of the day how accurate their information is, in fact many source tell you NOT to use it or employment purposes. It is better to use at two sources and corroborate results, the sources should be checked every six months at a minimum for accuracy through a background check audit using a known person, and last but not least the information must be vetted if a negative decision is going to be made based upon those reports.*

Common Issues that commonly cause "problems" with employee investigations:

- **Communication:** *The lines of communication should be set clear at onset of investigation and then confidentiality maintained. If at some point in the future there needs to be a deviation from the original plan of communication due to a development in the investigation this should be discussed and agreed upon with both legal and HR.*
- **Biased Perception & Conflict of interest:** *These usually results of being investigated by an in-house investigator, or the basic fact finding is taken into a full blown investigation process by a manager without approval or awareness of HR or legal, many times the supervisor is not even aware they have even done such an act. Once the initial fact finding is done in-house the only way to truly avoid these two issues is to use outside third party resources and train manager/supervisors when to stop questioning or probing into matters and turn it over to HR or legal.*
- **Using Technology:** *There are very strict laws about electronics to monitor people's activities as an employer. Legal must be involved in case law review, State & Federal statutes regarding such practices. The other actions that must be taken in this are that the employees expectation of privacy through policy, employee manual, s.o.p's etc must be clear and consistent.*
- **Lack Policy/Procedures:** *Stated as related to employee privacy expectations & right to investigate; especially in the hiring process in using FCRA and FACTA compliant forms*.
- **Collective Bargaining:** *Unions, not knowing what the members rights are under collective bargaining agreements*
- **General Lack of Knowledge:** *Oops. A lack of experience, communication between management, upper management, HR & legal.*
- **Superficial or Incomplete Investigation (or the appearance of one:** *This usually occurs out of a lack of experience, the sole use of in-house resources, or apathy. This must be avoided by having a clearly communicated investigative plan with all team members in agreement and on the same path of process.*

Example of how important doing a complete investigation can be:

Other interesting example of investigations can be a liability: EEOC v. CRST Van Expedited Inc., No. 07-CV-95-LRR (Feb. 9, 2010).

The U.S. Equal Employment Opportunity Commission (EEOC) was socked with $4.56 million in attorneys' fees, expenses and costs in a harassment case for the agency's failure to investigate the specific allegations of supposed harassment victims before it filed a complaint on their behalf.

In making the unusual award of fees to the prevailing defendant employer on Feb. 9, 2010, the U.S. District Court for the Northern District of Iowa described the EEOC's argument that several employees might have had meritorious claims as "a red herring." The court said that "the EEOC's failure to investigate and attempt to conciliate the individual claims constituted an unreasonable failure to satisfy Title VII's prerequisites to suit."

The court did deny the company's costs for videotaping depositions, agreeing with the EEOC that the employer could recover costs for stenographic transcripts or videotapes of depositions, not both, when the videotaped depositions were unnecessary. But the court awarded numerous other fees, including:

More than $4 million in attorneys' fees.
$242,212 for expert witness fees.
$119,185 for printing and copying expenses.
$62,183 in fees for the investigators CRST employed to locate and interview witnesses.
$34,135 for the travel expenses of the company's attorney.

The EEOC appealed the rulings in favor of CRST before the award of fees, but the district court asserted that it still could award fees, even while the substantive appeal is pending.

Best Practices in Employee Investigations:

Pre-Event:

1.) Have a clear working definitions crafted together with HR and legal working together about the company's position between an "inquiry" and an "investigation".
2.) Have HR and legal establish an agreed clearly defined parameter of when an inquiry ends and investigation begins.
3.) Working together legal and HR should establish a management policy that defines WHO can inquire, WHO can investigate and how either of these activities get's triggered and when.
4.) Have clear employee privacy policies in place within the employee manual that protect the company's interest in needing to investigate.
5.) Have FCRA & FACTA complaint forms crafted into the hiring process.
6.) Establish the **core team** that will be involved with most investigations. Suggested: Legal, HR, Third party investigator(s), and Risk Manager.
7.) Be sure that the company has a solid process of maintain documentation and consistent, fair, and honest employee evaluations.
8.) Develop your resource list ahead of time for outside investigative related vendors. Develop a relationship with them that allows for phone consultations and to bounce ideas off before triggering investigations. Be cautious of using only one resource for all investigative matters requiring an outside investigator.

Investigative Event:

1.) Be sure that there is a clear line of when an inquiry ends and an investigation begins.
2.) Before moving forward with actual investigation double check employee file to be sure the FRCA & FACTA complaint forms have been signed by the employee.
3.) Decide and/or choose outside investigative resource for the case. (Be sure to be aware of what privilege is needed in case the investigators activity needs such protection as this may bring in the need of outside legal counsel.)
4.) Meet with core team and execute the following: define purpose, scope, and parameters of investigation, establish who gets communication on the investigation and who does not, be clear about how investigation is being reported (verbal or written report) and to whom it being reported to and when (this should be the person internally managing the case from the employment side).

Post Investigation:

1.) Gather all reports and evidence from investigation.
2.) Have a meeting with the core team to review the results of the investigation.
3.) Decide on a course action related to the employee and matter in question.
4.) Document through meeting notes evidence considered and why decisions are made for employee file.
5.) Debrief investigative process and investigator(s).

Other points:

*Know the five main types of evidence needed in investigations and that can be used against an employer in litigation over an investigation. These are: Testimonial, Documentary, Statistical, Digital/Electronic, and Physical.

*Understand that the investigative field has changed drastically over the years. Now there are different types of investigators that are either qualified or not qualified to do certain things. Also companies need to vett their vendor to be sure they have proper state licensing, E&O insurance, and certifications to do the work activity requested.

Washington State Investigator information can be found at: http://www.dol.wa.gov/business/pi/
Washington also has a professional organization for investigators: http://www.wali.org/

Oregon State Investigator information can be found at:
http://www.oregon.gov/dpsst/PS/Pages/PSstatusandpublicrecords.aspx
Oregon also has a professional organization for investigators: http://www.oali.org/index.php

*Again, have proper hiring documentation in place that allows for maximum employer related investigative activity if needed (FCRA & FATCA compliant forms)

*Maintaining following policies/procedures consistently across the board. This is a matter of culture and training from the top down.

*Again, maintain accurate, complete, and honest evaluation records. It is important to maintain complete & thorough records of all employee file related matters.

*Respond to all complaints quickly, thoroughly, professionally & in consistent manner as set forth in inquiry and investigative protocol. (Take them seriously)

*And again, have your resources in place ahead of time for when needed.

QUESTIONS OR TO GET COST FREE FCRA/FACTA COMPLIANT FORMS CAN BE SUBMITTED:

STEVEY@3TIERSERVICES.COM OR 503-507-0468