Pre-employment Screening: Part Three

Background Investigations: Is Your Organization Prepared?

How does the Fair Credit Reporting Act, and other similar legislation, effect investigation into the activities of a current employee? What issues surround internal investigations?

In this, the final issue of the Background Investigations series, we discuss how the Fair Credit Reporting Act (FCRA) impacts internal investigation procedures. In addition, this article explores several other issues e.g. privacy, employee rights, and voluntary disclosure and how these principles govern an employer's activity. Briefly stated, every company has the right to investigate employee action and it is often in the employer's best interest to discover and report misconduct. As a general rule, the law does not require disclosure of an employee's unlawful conduct; however, under the Federal Sentencing Guidelines (FSG) for Organizations, which took effect November 1, 1991, corporations accused of misconduct can obtain substantial fine reductions based in part on the corporation's self-reporting efforts. So, companies are well incentivized to ferret out and report misconduct. Every organization conducts internal investigations but few properly understand the complex interlacing of governing issues, issues like privacy and access rights, reporting requirements, and the pros and cons of voluntary disclosure. A discussion of these and other relevant topics follows.

Impact of the FCRA

Understanding the revised Fair Credit Reporting Act ("FCRA") and its implications is critical to conducting lawful internal investigations. No longer is the notion of conducting purely "internal" investigations into employee misconduct a shield to the demanding authorization, notice, and reporting requirements of the Act. The revised FCRA presents significant hurdles to be overcome by internal investigators. For example, under the FCRA any individual or organization requesting a consumer report must notify the subject of its intent to obtain the report. Thus, the notice requirement prescribed by the rule gives targeted employees the opportunity to alter or destroy evidence, and to line up accomplices in a cover-up scheme.'

But the revised FCRA does not handcuff careful investigators and strikes a proper balance between employer needs and employee rights. Congress revised the FCRA in 1996 in part to curb the abuses made possible by the explosion in technology-related data collection. Originally passed in 1973, the FCRA was intended to standardize the financial credit reporting process and ensure that equal access and anti-discrimination laws could be enforced. The 1996 revisions extended the Act from financial records repositories used in credit decisions and similar transactions, to cover any repository where an individual's records are compiled, maintained, and reviewed. Importantly, the revised FCRA expanded the definition of "consumer report" to include background investigations reports, personnel and HR data collection, witness statements, and any other report or collection of data pertaining to an individual.

Under the revised FCRA there are three significant concerns investigators must address to conduct successful internal investigations:

Authorization: No individual or organization may obtain a consumer report without first receiving the subject's authorization before proceeding. Investigators cringe at the very notion of alerting targeted individuals by seeking their permission to investigate, but compliance doesn't necessarily spell

disaster. Federal Trade Commission opinion make it clear that organizations can obtain blanket authorization from all employees, provided that such authorization is specific, separate, and includes a list of the employee's rights. Optimally, employers meet authorization requirements by having all new employees sign an investigative authorization form upon hiring. One that indicates the employee's acquiescence to background checks, credit checks, and access to personal data collection pools. Standard release clauses present in most employee applications, however, are rarely sufficient. The authorization form must be a separate document specifically releasing background information accompanied by an explanation of the employee's rights to review and respond to any such information, as well as any recourse the employee may have in case of abuse. Still, organizations, which have not required such authorization upon hiring, need not view compliance as a threat to their ability to investigate employee misconduct. The same blanket release can be obtained retroactively. Granted, implementation of company-wide policy authorizing investigations may ruffle a few feathers, but the intent underlying the revised FCRA serves as a smoothing factor. The FCRA rules exist to protect employees from abuse, so retroactive authorization need not be viewed as an organizational invasion of privacy, but rather an organizational effort to cabin investigative authority both to protect employees' rights and to protect the organization.

Notice: FCRA notification requirements tend to be viewed as the most dangerous issue with regard to conducting internal investigations largely because this section of the revised law is widely misunderstood! The FCRA requires that any employer who desires to take adverse action against an employee provide that employee with an unedited copy of the report(s) on which the decision to take such action is based.

Investigations run above board usually will not run afoul of notice requirements. Assuming an organization has authorization to proceed with an investigation, notice is no bar to fully compliant, successful investigations. If an organization gathers information and determines that misconduct requiring adverse action has occurred, the organization simply notifies the employee and provides copies of the underlying data. If the employee accepts the organization's decision, the matter is essentially closed. If, however, the employee takes issue with the underlying data, the FCRA reporting provisions apply.

Reporting: Reporting represents the most critical element for FCRA compliance. This is the most vital adjustment under the new rules. Since reports used in investigations and any findings made therein are more easily discoverable (requiring only the request of the individual), it is critical that investigators' reports be factual, accurate, complete, and balanced. The validity of any decision based on an internal investigation will be measured by the information contained in investigative reports. Any challenge to such a company decision will come against the strength, accuracy, and reliability of the underlying documentation. The company is best served by making an accounting of its investigation that appears inherently reasonable without further input or comment from the company. Besides the presumptive validity afforded complete investigative reports, the company stands to protect itself from collateral attack against its investigative procedures by virtue of the fact that its fully compliant procedures are outlined for the record. This latter approach contemplates future litigation, and so derives its benefit, but in the context of possible adverse action, anticipating litigation is a sound strategy.

The authorization, notice and reporting requirements of the revised FCRA codify what in many cases are standard business practices. And in those instances where companies must alter behavior to conform, the path between existing procedures and compliant procedures is likely to be short. Companies familiar with litigation in any form are sophisticated enough to seek authorization for

potentially "invasive" activities, notify employees of suspected misconduct, affording the accused an opportunity to respond, and document procedures on which it may take further adverse action. So the FCRA, while expansive in defining "consumer reports," is not an impediment to properly conducted internal investigations. Care, foresight, and common sense will guide most organizations through the seemingly complex FCRA requirements. Avoiding entanglement with the FCRA can also be accomplished by:

• Hiring and training specialized investigators;
• Partnering with qualified external investigators; and
• Farming all investigative work out to professional investigators.

The FCRA is not without its pitfalls. As Jonathan Turner points out in his work entitled “How to Run Investigations Under the Revised FCRA”, deliberate compliance with FCRA provisions potentially conflicts with investigative situations “involving certain narcotics, sexual harassment, OSHA regulations, and other types of actions...[t]he potential chilling effect of [which] has not yet been tested in court.” So companies, and in particular investigators, must stay on their toes as the law develops in these related fields. The most advisable course of action is to stay abreast of developing state and federal law. Study the decisions of the courts as they resolve these underlying conflicts so as to avoid emulating the companies you're reading about.

Of course, compliance with the FCRA cannot stand as an independent concern for internal investigators because inextricably intertwined with FCRA authorization, notice, and reporting requirements are the employee's expectation of privacy in the workplace, and the investigator's methodologies in conducting workplace inquiries. The remainder of this article attempts to highlight some of those concerns and how they fit into successful internal investigation programs.

Expectation of Privacy in a Corporate Environment

Internal investigators constantly run up against invasion of privacy claims when looking into employee misconduct. Investigators are buttressed, however, by the mantra running through the prevailing jurisprudence regarding workplace privacy expectations: basically there are none. This, of course, should not be read as an employer's unfettered right to investigate any work-related aspect of an employee.

Courts that have addressed the issue of employees' expectations of privacy with respect to voice mail and e-mail communications, for example, have focused on whether the employer had a written policy on the subject. In deciding these cases, courts have considered whether the policy informed employees that electronic communications were stored and could be accessed by supervisors, and whether the employees gave a written acknowledgment that they received the policy. Under these circumstances courts have found that the employees possess no reasonable expectation of privacy!

Investigators must understand the organization's privacy policy as a factual predicate to conducting investigations. In an invasion-of-privacy claim arising from a workplace investigation, as in a Fourth Amendment claim, employees may allege that their employers violated their legitimate “expectation of privacy”. As an example, consider K-Mart v. Trotti, where an employee maintained a reasonable expectation of privacy in a locker that the employee had locked at her own expense with the employer's consent. The Trotti court focused on two key facts: (1) that the employee purchased the lock; and (2) that the employer was aware of the personal lock, did not object, and so manifested its consent to the employee's expectation of privacy in the locker. In a situation such as this, an

investigator seeking to discover the contents of the locker would violate the employee's privacy rights by opening and searching the locker. It follows from the Trotti decision, that the expectation of privacy would not have been reasonable if either the company provided the lock or had in place a policy prohibiting the use of personal locks on company equipment. In that instance, the investigator would be authorized to search the locker.

The lesson here is that company policy often dictates the level of privacy employees may reasonably expect. Investigators must understand both the intent of the organization drafting the policy and the likely interpretation that policy will receive in court in order to protect the validity of the investigation and avoid subjecting the organization to liability.

Employee Rights

Similarly, investigators must be aware of the employee's rights with respect to investigative proceedings. In addition to those rights defined and protected by the FCRA or Fourth Amendment privacy protections, employee's retain certain rights as defined by the National Labor Relations Board. In unionized settings, a union employee has the right to have a union representative present, upon request, during an investigative interview that the employee reasonably believes may result in discipline." This so-called "Weingarten right," named after the U.S. Supreme Court's decision in NLRB v. Weingarten, Inc., specifically prevents union employers from questioning union members without representation. The Weingarten right has been extended to protect nonunion employees as well, and prescribes a non-union employee's right to have a co-worker present during “investigative interviews”. Strict reading of the Weingarten right places the burden of requesting representation on the employee, and so organizations are not obligated to either provide representation or inform employees of their right to be represented. However, a request for representation must be complied with immediately for failure to provide requested representation or threatening adverse action based on an employee's refusal to participate without representation subjects an employer to unfair labor practice claims.

Investigators prompted by urgency may seek to interview an employee about a subject related to the investigation whether that employee is the target of the investigation or not. A carefully trained investigator will only do so where such inquiries do not raise prospective unfair labor practice claims.

Adverse Action

Last among the substantive issues regarding internal investigations are the procedures precipitating post-investigation adverse action by the employer. Investigations resulting in adverse employment actions raise a number of legal issues, and potentially serious pitfalls for the internal auditor beyond those evident under the FCRA. Chief among them is the employer-employee relationship.
If an employer contemplates possible adverse action as a result of suspected employee misconduct, the investigator must be aware of the nature of the employment relationship. In the case of contract employees, the terms of the contract may well impact how an organization proceeds. For example, some contracts specify termination dates, and the company's best option may be to let the contract expire rather than battle over wrongful dismissal claims. Other contracts specify that employment will continue until an event or events occur. Is the underlying event sufficient to satisfy the contract's termination clauses?

In the absence of a written employment contract, courts have looked to other items to find the existence of an implied agreement for a definite term; for example a statement in an “employee

handbook". What concerns the employer is identifying the express or implied term and deciding whether the underlying action raises sufficient cause for dismissal under such terms. In the absence of any employment agreement, most states recognize employment "at will" where an employee may resign or be terminated at any time, with or without cause. Even in such instances, most courts recognize several public policy exceptions prohibiting an employer from taking disciplinary action against an employee in retaliation for whistle-blowing, for example.

Lingering behind these decisions is the threat of wrongful dismissal suits, which burden even the most righteous organizations. Careful employers protect themselves against the ever-present threat of employment-based litigation utilizing several creative approaches. The "Notice Hearing" approach, long espoused in corporate America, includes both pre- and post-disciplinary hearings designed to put the employee on notice of the underlying charge and give the employee an opportunity to prepare a defense. Typically, the employee will receive a pre-disciplinary hearing where the employee will be notified of the charges, informed of the evidence supporting the charges, and given a chance to explain the underlying actions. Later, the employee will attend a formal proceeding supervised by a neutral party. The employee and the employer may call witnesses and offer other evidence, and of course, both parties may be represented by counsel.

Other companies use internal Alternative Dispute Resolution (ADR) under which employees agree to take their grievances to a committee of both workers and management that investigates and delivers a binding decision. ADR typically costs employers less time and money to resolve employment disputes, but is not right for every organization. Still other, and typically smaller, companies use a peer review system because it supports the employee and instills a sense of fairness.

Regardless of the approach, the investigator may find information related to his potential audience and prospective uses of investigative reports useful in outlining his investigative approach. In addition, as approaches vary, so to may corporate goals regarding investigative reports.

Technology and Methodologies Investigation

Internal investigators must also consider, develop, and select methodologies appropriate to their goals, and it is here where technology issues raise their ugly head implicating privacy concerns and the FCRA's authorization, notice and reporting requirements.

Major corporations world wide now own, and are employing, technology allowing corporate security directors to secretly copy employee's hard drives and review files for evidence of misconduct. High-tech investigators at companies like Microsoft, Disney, Motorola, and Caterpillar use technology originally designed for law enforcement to catch corporate criminals.

The nascent computer forensics field is developing at a rapid pace, but already has outpaced even savvy computer user's computer autonomy. Forensics programs scan computer files in excruciating detail, revive deleted files, and look for data caches were even the most sophisticated computer operators would not.

One of the primary weapons in the hands of corporate security specialists, Encase, developed by Guidance Software Inc., was originally purchased by the U.S. Secret Service in 1998. Guidance subsequently received orders from dozens of federal and state law enforcement agencies, and now increasingly from the private sector. Its appeal flows from its ease of operation. Encase seeks out and copies a targeted drive without altering it, revives deleted files, then scans the copy for

predetermined "flags". The software operator determines which "flags" Encase will seek out everything from company trade secrets to proscribed Internet files. The program can search several PC's in mere hours, and takes a relatively short time to master. With a little training, Encase makes scanning hard drives a point-and-click procedure.

Companies employing such internal investigative techniques readily defend their actions, stating that "being able to retrieve computer evidence is essential to their ability to catch employees engaged in everything from spending too much time surfing the Internet to stealing company secrets. People don't always tell the truth about things, said Howard Schmidt, head of corporate security for Microsoft. "Their computers," he said, usually do.

Privacy advocates hail programs like Encase as a perfect tool for inappropriate snooping on employees' personal lives or smearing corporate whistleblowers. Companies enjoy an almost unrestricted right to electronically monitor employee activities. At the most basic level, workplace computers are considered company property, and as such employers are free to examine their contents without restriction. In fact, only in Connecticut are companies even required to inform employees if their computer use is monitored."

Voluntary Disclosure

A discussion of the pros and cons of voluntary disclosure is now warranted.

Advantages: First and foremost, voluntary disclosure may convince prosecutors to forego criminal prosecution, and go after the offending employee rather than the organization, or file lesser charges against the organization. Such consideration may well result in lesser or no criminal penalties, as well as the intangible benefit of avoiding criminal stigmatization. In addition, the Federal Sentencing Guidelines include voluntary disclosure as a mitigating factor in its penalty scheme, so even adjudicated organizations may benefit from disclosing internal misconduct. Finally, several government agencies, like the OIG, DOD, DOJ, and HHS, sponsor special voluntary disclosure programs with substantial rewards for organizations that report misconduct."

Disadvantages: Of course, voluntary disclosure of corporate misconduct brings with it the unfortunate possibility of alerting the government to crimes or other wrongdoing it might not otherwise have discovered. This risk weighs heavily on corporations as the penalties associated with corporate criminal liability are severe, and generally lead to even harsher civil penalties. In addition to fines and penalties, corporations face public stigmatization, loss of investor confidence, and possible exclusion from lucrative government contracting programs. Individuals potentially face fines and even jail time. Further, while certainly mitigating in terms of liability, voluntary disclosure does not guarantee immunity from prosecution assuring that self-reporting companies face significant risks with no guarantee of benefit."

Second, voluntary disclosure of corporate misconduct regarding government contracts potentially implicates the False Claims Act (FCA). Critical here is the possibility that corporations conducting internal investigations in preparation for voluntary disclosure face potential qui tam actions under the FCA. Employees participating in an internal investigation into corporate wrongdoing may become qui tam relators armed with enough information to put the company out of business.

Finally, voluntary disclosure typically results in waiver of the attorney-client privilege. Most notably this waiver of formerly privileged information potentially subjects the corporation to civil liability by third parties affected by the disclosure or the information disclosed.

In short, the company must weigh the pros and cons of voluntary disclosure, taking into account internal logic and current jurisprudence, before reporting internal misconduct.

Conclusion

By way of summation, internal investigators are constrained to act within a complex set of inter-related doctrines some easily identifiable, some less so.

The FCRA requires investigators to comply with strict authorization, notice, and reporting elements largely in place to protect employee's rights. In an interesting twist, compliance with the FCRA is the most concrete method available to protect employer's rights and avoid employer liability. But the FCRA is not the only governing body acting upon investigative procedures. The Fourth Amendment protects basic privacy rights, and investigators, though largely free to search within the workplace, must observe arguably inviolable Fourth Amendment protections. The National Labor Relations Board also contributes to the constraints placed on internal investigations by requiring employee representation in certain investigative settings. Lastly, the technology underlying investigative techniques can easily surpass the law's ability to monitor abusive conduct, and so investigators must be aware of how investigative tools likely effect investigative outcomes.

Despite the seemingly nebulous regulatory web surrounding internal investigations, an objective informed review illustrates that proscribed activity usually falls outside standard, legitimate business practice. In that sense, common sense and a touch of sophistication may well be the primary weapons in the arsenal of an internal investigator attempting to balance the job's demands and the need to perform a demanding job in a lawful manner.