A Timely Analysis of Legal Developments

ASAP®

October 2011

New SOX Decision by the U.S. Department of Labor's ARB Expands Whistleblower Protection Yet Again, Including Protection for Theft from Employer's Computer System

By Edward Ellis and Jill Albrecht

In the case of an employee who admitted to stealing personal identifying information of coworkers and confidential business documents from the company computer system, the Department of Labor's Administrative Review Board (ARB) held recently that: (1) theft of confidential personal and corporate information may be protected activity, depending on the circumstances surrounding the theft; (2) the Sarbanes-Oxley Act's ("SOX") anti-retaliation provision protects employees who make disclosures to the Internal Revenue Service (IRS) under the IRS Whistleblower Rewards Program; and (3) an employee need not allege shareholder fraud for SOX protection to apply.

The ARB remanded *Vannoy v. Celanese Corp.*, ARB Case No. 09-118 (Sept. 28, 2011), to an Administrative Law Judge (ALJ) for an evidentiary hearing on whether the employee's admitted theft of data in violation of both company policy and a written confidentiality agreement was protected under SOX section 806.

Background

Celanese hired the complainant, Matthew Vannoy, to reconcile problems with the company's corporate employee expense reimbursement system, known internally as "the U.S. Bank Card program." In June 2005, the company retained a consultant that reviewed the U.S. Bank Card program and recommended that the company implement a new electronic reimbursement system. Company management recognized throughout 2005 and 2006 that the U.S. Bank Card program was not working correctly. In December 2006, the company implemented the new system recommended by the consultant. The complainant was involved in the evaluation of the old system and the implementation of the new one. His job also included securing necessary information to substantiate expense reports. The complainant allegedly appeared to be aggressive in his dealings with employees submitting expense documentation that he found inadequate, and he ended up in several confrontations with employees about expense reimbursements. He was counseled to refrain from engaging in confrontational behavior with employee cardholders and to report serious disagreements to his supervisor.

In February 2007, after the new and improved expense reimbursement system had been implemented, the complainant filed an internal complaint, pursuant to the Celanese Business

Conduct Policy, alleging misuse and abuse of employee credit cards and describing the financial risk he thought the old system posed for the company. He also consulted an attorney. In April of that year, the complainant went on a short-term disability leave.

While he was on leave, the company decided to phase out certain U.S. finance positions, including the complainant's position and his entire department, and relocate it to Budapest, Hungary. The complainant was offered a retention agreement and stipend if he remained with the company through the transition, which the company expected to take between six and 18 months. The complainant agreed to stay for the bonus and returned from leave in October 2007. Due to his prior problems interacting with employee cardholders, he was instructed to refer any confrontational communications he received from employees seeking expense reimbursement to his supervisor. The complainant violated these instructions by continuing to engage in inappropriate communication with other Celanese employees.

In June 2007, while on leave, the complainant filed, through his attorney, a disclosure under the IRS Whistleblower Rewards Program that included 33 proprietary and confidential documents. The company was unaware of the complainant's IRS disclosure. In late October 2007, after a complaint from an employee who was dealing with the complainant about an expense reimbursement, the complainant's supervisor and another administrator decided to review the complainant's "sent emails" to determine whether he had continued to send inappropriate messages to cardholders despite having received a prior warning. In the course of this review, the managers discovered that the complainant had sent a document containing 1,600 unique Social Security numbers of current and former Celanese employees to his personal email account. The complainant later admitted during his deposition that he had turned this information over to the IRS in support of his IRS disclosure. The complainant testified that he was aware of the confidential nature of this information and admitted that he had previously agreed to the company's confidentiality agreement. He also admitted taking confidential business information in addition to the Social Security information of employees.

On November 5, 2007, the complainant was suspended without pay. On November 8, 2007, he supplemented his internal Business Conduct Policy complaint. The company investigated the complainant's complaint, but the complainant refused twice to provide information as part of the investigation. He was subsequently terminated in January 2008 for violation of the company's confidentiality policy. The company turned the theft problem over to the local prosecuting authorities, but the complainant was not charged with any crime. On February 5, 2008, the company sent the complainant a letter outlining the investigatory findings and describing the steps that the company, on an ongoing basis, was undertaking to correct any issues. In March 2008, the complainant's department was transitioned to Hungary as planned.

The ARB Reverses Summary Judgment for the Company

The complainant filed a complaint with the Occupational Safety and Health Administration (OSHA) alleging that the company violated Title VIII of the Sarbanes-Oxley Act of 2002, 18 U.S.C. section 1514A, when it terminated his employment. OSHA dismissed the complaint. The complainant then requested a hearing before an Administrative Law Judge and filed an amended complaint. Celanese moved for summary decision, which the ALJ granted.

The ARB decision reversing and remanding to the ALJ contains three principal holdings of interest to employers.

First, the ARB reiterated its holding in *Sylvester v. Parexel Int'l, LLC*, ARB No. 07-12 (May 25, 2011), that an employee need not complain about shareholder fraud to state a claim under SOX, nor need he allege that the subject of his complaint was material to the company's financial statements. Thus, the ARB appears to have given life to many employers' concerns that, after *Parexel*, an employee's complaint about his coworker's or boss's expense account could be construed as a whistleblowing event that triggers SOX protection.

Second, the ARB held that the language of 18 U.S.C. section 1514A(a)(1)(A) setting forth protections for an employee who has provided information to "a Federal regulatory or law enforcement agency" applies to employees who report tax fraud to the IRS under the IRS Whistleblower Program. This no doubt comes as a surprise to many attorneys who considered SOX a shareholder fraud statute and the SOX whistleblower protection applicable only to reports made to the Securities and Exchange Commission (SEC) or the criminal authorities that enforce the shareholder fraud statutes.

Third, using some legislative history from SOX and its own take on the Congressional purpose behind the Dodd-Frank Act for support, the ARB suggested that theft of documents in the service of law enforcement might be protected activity under SOX. Recognizing the "clear tension between a company's legitimate business policies protecting confidential information and the whistleblower bounty programs," the

ARB remanded the case to the ALJ for a hearing on: (1) whether the confidential information the complainant stole was the kind of "original information" that Congress intended to protect under the IRS Whistleblower Program and the Dodd-Frank Act; and (2) whether the manner of the transfer of the information was protected under SOX. The ARB emphasized that the SOX legislative history suggests that Congress intended to protect "lawful acts to disclose information." This case, of course, is a SOX case and "original information" is a Dodd-Frank concept not mentioned in SOX. It appears that the ARB considers the collection of information to be protected under SOX if the information satisfies the Dodd-Frank definition of "original information" and the manner in which the information was collected and transmitted is not unlawful.

Missing from the ARB analysis are two concepts. The first missing concept is that of a balancing test. The ARB makes no effort to balance the employer's need to adopt "legitimate business policies" against the whistleblower's right to collect information to support a SOX claim. Federal retaliation law has always required a balancing test when a court is confronted with an employee who uses extreme methods to participate in an agency proceeding or to oppose unlawful practices. One of the earliest and best known cases is *O'Day v. McDonnell Douglas Helicopter Co.*,[1] in which the plaintiff stole confidential documents from the company to support a discrimination lawsuit. The employer fired the plaintiff for the theft, and he claimed it was a protected activity. The Ninth Circuit applied a balancing test to determine whether an employee's conduct was protected. In upholding summary judgment for the employer, the court stated:

> In balancing an employer's interest in maintaining a "harmonious and efficient" workplace with the protections of the anti-discrimination laws, we are loathe [sic] to provide employees an incentive to rifle through confidential files looking for evidence that might come in handy in later litigation. The opposition clause protects reasonable attempts to contest an employer's discriminatory practices; it is not an insurance policy, a license to flaunt company rules or an invitation to dishonest behavior.[2]

Aside from its reference to "lawful acts" drawn from the legislative history of SOX, however, the ARB recognizes no limit on the protection provided to a whistleblower's efforts to spy on the employer.

The second concept missing from the ARB's opinion is that of criminal activity. The fact that the complainant was not prosecuted does not make his behavior lawful. As it is described in the ARB's decision, the complainant's conduct may have violated the Computer Fraud and Abuse Act and possibly other laws against stealing personal identifying information. Yet, the ARB did not provide guidance on the question of unlawful activity by the employee except to quote the legislative history. The IRS and the SEC have ways to obtain business information other than relying on employee theft.

Implications for Employers

It is easy to envision a scenario in which an employer wants to terminate a known whistleblower because the whistleblower is raiding the company computer system for evidence, even though the employer may face a claim for SOX or Dodd-Frank liability stemming from the termination. The employment consequences of the termination may simply be less unattractive than the commercial consequences of stolen business plans, financial data, or personnel information. If the ARB's position is that illegal acts by an employee are protected if they are in the furtherance of private sleuthing for the government, then employers lose the protection of laws on which they rely to safeguard their business information. This issue bears watching in the coming months and years.

Edward Ellis is a Shareholder in Littler Mendelson's Philadelphia office, and Jill Albrecht is an Associate in the Pittsburgh office. If you would like further information, please contact your Littler attorney at 1.888.Littler or info@littler.com, Mr. Ellis at eellis@littler.com, or Ms. Albrecht at jalbrecht@littler.com.

---

[1] 79 F.3d 756 (9th Cir. 1996).

[2] *Id.* at 764. *Niswander v. Cincinnati Ins. Co.*, 529 F.3d 714 (6th Cir. 2008), and *JDS Uniphase v. Jennings*, 473 F. Supp. 2d 697 (E.D. Va. 2007), reach similar conclusions.