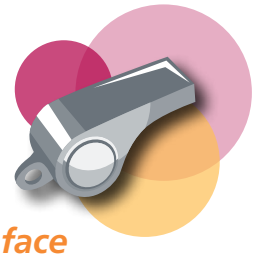
SEYFARTH SHAW LLP
ATTORNEYS

Workplace Whistleblower



Perspectives on whistleblower situations that employers frequently face

An Employee is Stealing Company Documents… That Can't Be Protected Activity, Right?

Hypothetical, based upon a real fact pattern: A supervisor discovers that an employee has recently downloaded thousands of pages of confidential Company billing and financial information, and e-mailed it to her personal e-mail address. Upon further investigation, the supervisor discovers that the employee has asked other employees to also send Company documents to her personal e-mail address.

What Should the Company do?

In coordination with legal counsel, the Company will need to undertake an immediate internal investigation of the employee's activities. The Company should review the information that was taken and determine whether the information was already publically available or whether it contains Company confidential or trade secret information. Additionally, the Company should determine whether multiple copies of the stolen documents exist and whether they have been designated or labeled as confidential or trade secret. The Company should evaluate its internal policies and procedures as well as its agreements with the employee to determine the scope of the employee's violations as well as determine whether the employee has a history of similar violations or conduct. If so, hopefully those prior violations are documented.

The Company should involve its internal IT Security department or an outside IT security/forensic specialist to assess and remedy the data breach, and ensure that the Company has a full understanding of what data and/or documents were accessed and transferred, as well as to preserve the electronic evidence of the incident. Interviews of employees, including those employees from which the employee at issue attempted to solicit further documents, should be conducted to determine whether Company documents were actually provided to the employee, as well as to attempt to uncover the motivations for the employee's actions. If other employees transferred documents to the employee, an investigation of their activities will be necessary. Additionally, depending upon the nature of the information taken by the employee(s) and any contractual obligations implicated, the Company may have an obligation to report a data breach, particularly if the employee has shared the purloined data with unauthorized third parties.

The Company should contact the employee and conduct an immediate in-person interview. During the interview, the employee should be confronted regarding the data transfers. The Company should determine whether there is an innocent explanation for the activity, as well as staying mindful of and adhering to its own whistleblower protection policies. The Company should probe the extent of the personal transfers, transfers from others, and whether the employee has disclosed the documents to third parties. The Company should also question the employee concerning the employee's motivations as well as the employee's awareness of Company policies and agreements prohibiting such activities. The Company should attempt to obtain concessions that the employee's actions violate the Company's policies/agreements. The Company should ask for the employee's immediate cooperation in returning the data and request access to the employee's personal email account as well as any other electronic devices or accounts that contain Company information to accomplish the same. It is

important that the Company obtain the return of the data, particularly if the information is confidential or trade secret, so that the Company can attempt to preserve its confidential nature.

Assuming that there is no legitimate reason for the employee's actions, the Company will need to consider appropriate discipline for the situation, including considering suspension or termination of the employee. The Company should have written documentation clearly demonstrating the reason for such discipline was for violation(s) of particular policies or agreements, not in retaliation for any purported whistleblowing. Civil legal theories against the employee may include, among other claims, breach of contract, breach of loyalty, conversion, trade secret misappropriation, and/or a violation of the Computer Fraud and Abuse Act (depending upon the jurisdiction) or similar state computer data protection or access laws. Depending upon the gravity of the situation, the Company may also want to consider approaching law enforcement to consider pressing charges against the employee. If the employee refuses to return the documents and make the employee's accounts and other electronic devices/accounts containing Company data available for inspection to obtain the return of the purloined data, the Company may need to consider seeking immediate injunctive relief in court.

Before taking any adverse actions against the employee, however, the Company needs to evaluate the employee's potential claims against the Company and any whistleblower protections for self-help discovery in the particular jurisdiction. For instance, in the SOX whistleblower case *Vannoy v. Celanese Corp.*, No. 09-1118, 2011 DOLSOX LEXIS 68 (ARB Sept. 28, 2011), the Department of Labor's Administrative Review Board recognized the tension between legitimate employer confidential policies and employee whistleblower bounty programs, like the provisions in Dodd-Frank that preclude companies from enforcing or threatening to enforce confidentiality agreements to prevent whistleblowers from cooperating with the SEC. The ARB, relying on Internal Revenue Service and SEC whistleblower bounty programs, reversed an ALJ's finding in favor of the employer and remanded the matter for evidentiary hearing to determine whether the employee's taking of company documents by sending them to his personal email account was protected lawful conduct within the scope of SOX.

Similarly in, *Quinlan v. Curtiss-Wright Corp*., 204 N.J. 239 (N.J. Dec. 2, 2010), the New Jersey Supreme Court, employed a seven factor test to determine the propriety of an employee's taking of company documents to support her legal claims. "The ultimate question under the balancing test is whether the employee's dissemination of confidential documents was reasonable under the circumstances. This type of test is consistent with the general notion that oppositional activity must be reasonable in order to receive protection under Title VII and other similar statutes." In upholding a ten million dollar verdict against the employer, the court found that employer could have terminated plaintiff for taking the documents but not for her counsel's use of the performance review in deposition. The court further found that the plaintiff's attorney's use of the comparator's performance review at deposition was the actual reason for her discharge, and thus plaintiff was indeed discharged for engaging in protected activity. In reaching its decision, the court found the factors supporting plaintiff's position were that plaintiff gave the performance review only to her attorneys, it was directly relevant to her claim, she had a colorable basis to believe that the performance review would not have been disclosed during discovery, and the disclosure of the document was not disruptive because its disclosure did not threaten the operation of the company in any way.

In contrast, in *O'Day v. McDonnell Douglas Helicopter Co.*, 79 F.3d 756 (9th Cir. 1996), the Ninth Circuit rejected the plaintiff's age discrimination claim based upon plaintiff's theft of documents he found by rummaging through files in his supervisor's office on the night he was denied the promotion. "In balancing an employer's interest in maintaining a 'harmonious and efficient' workplace with the protections of the anti-discrimination laws, we are loathe 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." The Sixth Circuit reached a similar result in *Niswander v. Cincinnati Ins. Co.*, 529 F.3d 714, 718 (6th Cir. 2008).

In sum, courts addressing employee self-help discovery in whistleblower cases have reached differing results across the country. This reality provides Companies with a cautionary message: don't accept the theft of Company documents in violation of Company policies and agreements but tailor your approach to fit the employee's specific claims and your jurisdiction's discovery self-help laws. Courts in whistleblower cases have generally analyzed six factors to determine whether the self-help taking of Company confidential documents is reasonable: (1) how the documents were obtained; (2) to whom the documents were given; (3) the content of the documents; (4) whether the documents were produced in response to a

discovery request; (5) the scope of the employer's confidentiality policies/agreements; and (6) the necessity to preserve the evidence by the employee. As evidenced by *Vannoy*, special attention should be given to the employee's specific potential whistleblower claims as certain claims such as SOX claims may provide protection to take certain Company documents (or at a minimum divulge Company information), particularly if such information is shared with the SEC. Companies should have broad and comprehensive confidentiality policies, which are widely communicated and uniformly enforced and specific care should be given to mark documents as confidential and limit confidential documents on a need to know basis. Careful screening of job candidates and the consistent use of effective entrance and exit interviews are essential. Companies should also consider using data protection software which provides alerts regarding large data transfers by employees, limits the size of data transfers, and blocks specified computer activities, including access to select websites, including file-sharing sites, and/or limits or restricts use of USB devices.

For more information on this important topic, please see our previously recorded webinar entitled *Employee Theft of Trade Secrets or Confidential Information in Name of Protected Whistleblowing*.

By: *Robert Milligan*

Robert Milligan is a partner Seyfarth's Los Angeles - Century City office. If you would like further information or to submit a question regarding this post please contact the Whistleblower Team at *ask-whistleblower@seyfarth.com*.

Attorney Advertising. This One Minute Memo is a periodical publication of Seyfarth Shaw LLP and should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have. Any tax information or written tax advice contained herein (including any attachments) is not intended to be and cannot be used by any taxpayer for the purpose of avoiding tax penalties that may be imposed on the taxpayer. (The foregoing legend has been affixed pursuant to U.S. Treasury Regulations governing tax practice.) © 2013 Seyfarth Shaw LLP. All rights reserved.