Purloined Documents, Confidential Employer Data, and Counterclaims in Whistleblower Retaliation Cases[1]

by
David J. Marshall and Abigail Cook-Mack[2]
Katz, Marshall & Banks, LLP
1718 Connecticut Ave., N.W.
Sixth Floor
Washington, DC 20009
(202) 299-1140
www.kmblegal.com

presented at the

Fall 2013 Seminar of the
National Employment Lawyers Association

Shining the Light on Whistleblower and Retaliation Claims

Washington, D.C.
October 18 - 19, 2013

 This is the fourth revision of a paper originally presented in 2010.

[2] David J. Marshall is a partner with Katz, Marshall & Banks, LLP, in Washington, D.C. The firm specializes in the representation of plaintiffs and relators in whistleblower cases, employment disputes, and civil rights and civil liberties matters. Abigail Cook-Mack is an associate with the firm.

Every attorney who represents whistleblowers is familiar with this scenario: you walk into the conference room to meet with a prospective client who has told you about her whistleblower retaliation case over the phone, and you find her thumbing through an eight-inch stack of documents that she has placed on your conference table. As the prospective client relays the facts to you, she begins reaching into the stack and handing you documents that appear to provide strong support for a claim of unlawful retaliation.

Your prospective client may show you a recent internal memorandum documenting high-level concern about the accuracy of her company's earnings statements – a concern that she, as an accountant, had reported to the auditors just two days before the company placed her on a performance improvement plan. She may have been fired after complaining of safety issues as an engineer at a nuclear power plant, and hands you a letter showing that her bosses were trying to hide the problem until they could fix it more easily during a scheduled refueling outage. Or she may have learned that her employer has been defrauding the federal government out of millions of dollars per year, and she has brought you a banker's box of billing records she dug up to prove it.

As a plaintiffs' lawyer, you can't help getting excited when you hold a piece of hard evidence in your hand, but you also have to realize that the situation may be more complicated than it appears. How did your new client obtain these documents? Do the documents contain trade secrets, attorney-client communications, or confidential customer information? Did she have legitimate access to the documents, did she jimmy a file cabinet to get at them, or did she do something in between? And even if her access was legitimate or authorized, did she sign a

confidentiality agreement prohibiting her from showing them to you and obligating her to return them upon termination?

Depending on the answers to these and related questions, and on how you balance the risk and opportunity that is sitting in a stack on your conference table, you may have a winning whistleblower case or you may have a client who faces civil or even criminal liability. Given the stakes involved in the handling of client documents, an attorney representing whistleblowers needs to understand the legal and practical ramifications of a client's evidence-gathering actions in order to properly advise and represent the client. The effects emanating from a client's actions have grown many-fold in recent years, when nearly all businesses have begun storing their secrets and other information electronically, and when the proliferation of computer networking and inexpensive thumb drives has made it possible – often surprisingly easy – for employees to access their employers' most confidential information and remove from the workplace it by the virtual truckload. You also need to think about your own ethical obligations, which, depending on the document and the jurisdiction, may even require you to return the evidence to the employer.

This article addresses some key issues that arise when a whistleblower has acquired – or "purloined" if you ask the boss – documents or other information and provided them to her attorney for use in developing and prosecuting her case. Its purpose is not to provide a comprehensive analysis of the law in every jurisdiction, but rather to help the practitioner identify some potential pitfalls and steer around them where possible.

I. Document Acquisition and Dissemination as Protected Activity.

Employees who decide to speak out about improprieties often realize that documentary evidence will be essential in convincing management bodies, government regulators or law enforcement authorities that the concerns they raise are valid ones. Take the case of a finance employee at a publicly traded company who discovers that management is misrepresenting the company's financial condition in a manner that is so potentially catastrophic for shareholders that he is willing to risk his job to insist on full disclosure and a restatement of earnings. He reports it up the ladder but the higher-ups just brush him off. If he runs empty-handed to the Securities and Exchange Commission ("SEC"), the company may be able to cover up the violations before the regulators can investigate. However, if the employee takes emails, memoranda and test reports with him when he visits the SEC, it will not be a matter of his word against theirs. Corroborating documents may be even more critical in the case of a *qui tam* relator, who needs to plead his fraud allegations with a level of particularity that is better based on documents than on memory. For these and other reasons, whistleblowers often take advantage of their positions as employees to obtain documentary, physical or electronic evidence of their employers' unlawful activities.

While acquiring such evidence can help a whistleblower prove the wrongdoing, it also may provide the employer with a legitimate, non-retaliatory ground to suspend, terminate, or take other adverse actions against the employee. Courts have consistently held that anti-retaliation statutes do not protect employees who unreasonably appropriate records without

permission for the purpose of using them against the company.[3] This means that in many situations an employer can legally terminate a whistleblower for acquiring and disseminating confidential documents, even if the employee has engaged in protected activity by reporting misconduct and took the documents only to corroborate her allegations.

A. Balancing Test in Cases Under Title VII and Other Discrimination Statutes.

To determine if an employee's acquisition and dissemination of confidential documents itself qualifies as protected activity in discrimination and retaliation cases arising under Title VII, courts have historically applied a balancing test to determine if the employee's actions were reasonable under the circumstances. The Sixth Circuit explained in *Niswander v. Cincinnati Insurance Co.*:

> A balance must be achieved between the employer's recognized, legitimate need to maintain an orderly workplace and to protect confidential business and client information, and the equally compelling need of employees to be properly safeguarded against retaliatory actions. Allowing too much protection to employees for disclosing confidential information may perversely incentivize behavior that ought not be tolerated in the workplace – namely, the surreptitious theft of confidential documents as potential future ammunition should the employee eventually feel wronged by her employer. On the other hand, inadequate protection to employees might provide employers with a legally sanctioned reason to terminate an employee in retaliation for engaging in activity that Title VII and related statutes are designed to protect.

[3] *See, e.g., Laughlin v. Metro. Washington Airports Auth.*, 149 F.3d 253 (4th Cir. 1998) (taking documents from supervisor's desk and providing them to coworker for use in coworker's discrimination case is not protected oppositional activity under Title VII); *Jefferies v. Harris County Cnty Action Ass'n*, 615 F.2d 1025 (5th Cir. 1980) (copying and dissemination of employment records held not to constitute protected activity under Title VII where employee could not demonstrate failure of legitimate means for obtaining information); *Niswander v. Cincinnati Insurance Co*., 529 F.3d 714 (6th Cir. 2008) (knowing dissemination of confidential documents irrelevant to plaintiff's legal claims is not protected activity under Title VII's participation or opposition clauses); *O'Day v. McDonnell Douglas Helicopter Co.*, 79 F.3d 756 (9th Cir. 1996) (employee theft of sensitive personnel document for use in discrimination lawsuit did not constitute protected oppositional activity under federal age discrimination law).

529 F.3d 714, 722 (6th Cir. 2008); *see also Jefferies v. Harris County Community Action Ass'n*, 615 F.2d 1025, 1036 (5th Cir. 1980) ("[T]he courts have required that the employee conduct be reasonable in light of the circumstances, and have held that 'the employer's rights to run his business must be balanced against the rights of the employee to express his grievances and promote his own welfare.'") (internal citation omitted).

Jefferies v. Harris County Community Action Ass'n, an early and oft-cited case involving "purloined documents," illustrates the fact-specific approach most courts have taken when weighing the competing interests of employee and employer. 615 F.2d 1025 (5th Cir. 1980). Believing that she had been discriminated against as an employee of the Harris County Community Action Association, Jefferies copied relevant personnel materials that she found and then sent them to a member of the association's board of directors, presumably seeking corrective action. *Id.* at 1029. Instead of providing help to Jefferies, the board member reported the disclosure to Jefferies' supervisor, and an investigation commenced leading to Jefferies' termination. Jefferies argued, among other theories, that the association had discharged her in retaliation for engaging in protected activity – that is, her opposition to unlawful employment practices by disseminating documents that she believed evidenced discrimination.

Citing several factors that led it to conclude that Jefferies' actions were unreasonable under the circumstances, the court held that Jefferies had not engaged in protected activity. In particular, the court found that the association believed the personnel files were confidential and that their dissemination violated agency policy. *Id.* at 1036. The court also noted that Jefferies had acted at a time when the association had been growing increasingly concerned about the unauthorized dissemination of agency documents. *Id.*

In contrast to the organization's apparently legitimate interest in maintaining the confidentiality of personnel records, Jefferies was unable to demonstrate that the association's official grievance procedure was inadequate to address the alleged discrimination, or that the association would have destroyed the documents had she not taken action to preserve them. *Id.* These facts, the court found, undermined the plaintiff's argument that she needed to keep and disseminate documents that she might legitimately have obtained through the agency's grievance procedure or through civil discovery. *Id.*[4]

In *Niswander* the Sixth Circuit Court of Appeals fleshed out in detail the precise factors that courts should consider when attempting to balance, as *Jeffries* did, the competing interests of employees and employers. They include:

> (1) how the documents were obtained, (2) to whom the documents were produced, (3) the content of the documents, both in terms of the need to keep the information confidential and its relevance to the employee's claim of unlawful conduct, (4) why the documents were produced, including whether the production was in direct response to a discovery request, (5) the scope of the employer's privacy policy, and (6) the ability of the employee to preserve the evidence in a manner that does not violate the employer's privacy policy.

Id. at 726 (internal citations omitted).

The New Jersey Supreme Court recently expanded the six factors considered in *Niswander* to include a further factor, the strong remedial purpose of the New Jersey anti-discrimination statute. *See Quinlan v. Curtiss Wright Corp.*, 8 A.3d 209, 221 (N.J. 2010). The New Jersey judges determined that courts should "be cognizant of the broad remedial purposes the Legislature has advanced through our laws against discrimination … [and] must consider the

[4] Other courts have also found that the availability of discovery and other proper methods of obtaining documents can tip the scale towards the employer's interest in maintaining the confidentiality of its record. *See e.g.*, *Hodgson v. Texaco Inc.*, 440 F.2d 662 (5th Cir. 1971); *Hellman v. Weisberg*, 2007 WL 4218973, at *5 (D. Ariz. 2007), *aff'd* 360 Fed. Appx. 776 (9th Cir. 2009); *Dartey*, 82-ERA-2, slip op. at 7.

effect, if any, that either protecting the document by precluding its use or permitting it to be used will have upon the balance of legitimate rights of both employers and employees." *Quinlan v. Curtiss-Wright Corp.*, 8 A.3d 209, 228 (N.J. 2010). Although specific to New Jersey, this case could provide additional considerations for courts tackling the same challenges in future cases.

The analysis of these factors is necessarily a fact-specific one. In *Niswander*, the court placed significant emphasis on how the employee had obtained the documents and to whom the employee had distributed them. The court held that the plaintiff's dissemination of insurance claims records to her attorney did not constitute protected activity because she had searched through the records for the sole purpose of finding documents to support her retaliation claim. 529 F.3d at 727 ("Rather than innocently stumbling upon evidence of illegal employment practices, Niswander specifically searched through CIC documents that she had at her home office for the purpose of uncovering evidence of retaliation.").

Applying the same reasoning, the court in *Kempcke v. Monsanto Company*, 132 F.3d 442 (8th Cir. 1998), held that a jury could find that the plaintiff had engaged in protected activity when he gave his attorney documents evidencing age discrimination that he discovered and then refused to return. The court underscored the fact that Kempcke had "innocently" acquired the documents on the computer that Monsanto had issued to him. Unlike the plaintiffs in other cases in which courts refused to find their activities protected,[5] Kempcke had not engaged in surreptitious activities in order to uncover the inculpatory evidence. The court also implied that the fact that Kempcke had shared the documents with his attorney, and with no one else, was an

[5] *O'Day v. McDonnell Douglas Helicopter Co.*, 79 F.3d 756 (9th Cir. 1996) (plaintiff rummaged through supervisor's office); *Hellman*, 2007 WL 4218973 (plaintiff opened an envelope labeled "confidential" and disseminated the memorandum inside to coworker); *Dartey v. Zack Co. of Chicago*, 1982-ERA-2 (Sec'y Apr. 25, 1983) (nuclear whistleblower under the Energy Reorganization Act) (complainant took 15 personnel files from the company vault and tried to smuggle them off company premises).

important fact that could support a finding that Kempcke's actions were reasonable and thus protected.[6] *Id.* at 446-47. In *Johnston v. Donahoe* the district court of Arizona ruled against the employee focusing its attention on the fact that the content of the documents taken by the employee did not "substantiate the harassment claim," and were irrelevant to her claim of unlawful conduct. *Johnston v. Donahoe*, No. CV-10-01067-PHX-JRG, 2012 WL 1247204, at *5 D. Ariz. April 13, 2012).

Where an employee's dissemination of confidential documents is in violation of law or contrary to public policy, in addition to being contrary to the employer's interest, courts are even less likely to let the employee off the hook. In *Vaughn v. Epworth Villa*, 537 F.3d 1147, 1149, 53–54 (10th Cir. 2008), the Tenth Circuit held that the employer had a legitimate, non-retaliatory, and non-pretextual reason for the adverse employment action where the employee illegally supplied non-redacted medical records to the EEOC in support of her discrimination claim.

In addition, employees – at least those still employed – who use documents they have taken must take care to answer truthfully if asked where they obtained the documents. In *Collins v. Faurecia Interior Sys., Inc.*, 737 F.Supp.2d 792 (E.D. Mich. 2010), the plaintiff employee was an IT technician for the defendant employer. He used his position to access confidential Human Resources information relating to the company's investigation of his complaints, which he then used in mediation before the EEOC. *Id.* at 800. The employee then refused to reveal how he had obtained the confidential documents even after being warned he would be discharged if he did

[6] *But see Niswander*, 529 F.3d 714 (plaintiff's collection and dissemination of documents found not to be protected activity even though the plaintiff disseminated the documents only to her attorneys).

not answer. The court found that his termination was not a pretext for filing a discrimination charge but rather was due to his insubordination. *Id.* at 805-06.

B. Evidence-Gathering as Protected Activity in Connection with Certain Whistleblower Protections and Incentive Programs

Over the past few years, perhaps as a result of a growing recognition of the important roles whistleblowers play in our society, some courts and regulators have grown somewhat more accepting of the view that employees are justified in collecting documents for use in making whistleblower disclosures, and that they should be protected from retaliation for doing so. While this development is too limited to describe as a "trend," a plaintiffs' lawyer needs to be aware of important new protections for employees who face threats, firings or lawsuits as a result of evidence-gathering.

1. False Claims Act

Relators in *qui tam* actions under the False Claims Act ("FCA"), 31 U.S.C. § 3729, have a strong argument that the anti-fraud law's public policy of encouraging whistleblowers to come forward with evidence of wrongdoing elevates their evidence-gathering to the level of protected activity under the Act's anti-retaliation provision, 31 U.S.C. § 3730 (h). At least two courts have embraced this argument. In *United States ex rel. Grandeau v. Cancer Treatment Ctrs of America*, 350 F.Supp.2d 765, 773 (N.D. Ill. 2004), in which the *qui tam* relator copied and provided to government confidential documents that supported his *qui tam* claims, the court found that the relator did not breach his confidentiality agreement because disclosure to the government in *qui tam* actions was allowed under any circumstances. While the court did not elaborate on its reasoning, the decision supports the argument that the FCA has created such a well-defined and dominant public policy favoring employees who assist the government in its

investigation of fraud, and that the policy should outweigh any private agreement or employer policy that would effectively block such assistance, which is vital to the government's ability to uncover and prosecute fraud.

A federal court in the District of Columbia reached a similar result in *U.S. ex rel Head v. Kane Co.*, 668 F. Supp.2d 146, 152 (D.D.C. 2009). The court dismissed the former employer's counterclaims against the relator for breach of a confidentiality agreement by taking documents and providing them to the government as part of the relator's disclosures under the False Claims Act. The court stated that "[e]nforcing a private agreement that requires a *qui tam* plaintiff to turn over his or her copy of a document, which is likely to be needed as evidence at trial, to the defendant who is under investigation would unduly frustrate the purpose" of the False Claims Act's anti-retaliation provision. *Id.* Note that *Kane* dealt with a single email that contained direct evidence of the alleged fraud, and not with a broad array of confidential documents. *Id.* at 151-52.

While the FCA's anti-retaliation provision makes it clear that employers cannot lawfully retaliate against employees for investigating fraud on the federal government, *qui tam* practitioners would be mistaken to believe that the provision guarantees their clients blanket protection for removing and disseminating employer documents, even where the client subjectively believes he or she is investigating serious violations that would support a *qui tam* claim. This is especially true where, as it turns out, the *qui tam* claim is not sustainable and/or the FCA retaliation claim is weak for reasons unrelated to the employee's evidence-collection methods.

The risks associated with a plaintiff's collection and dissemination of documents in the FCA context are demonstrated in the recent case of *U.S. ex rel. Cafasso v. General Dynamics C4*

Sys., Inc., No. CV 06-1381, 2009 WL 1457036 (D. Ariz. May 21, 2009), *aff'd by* 637 F.3d 1047 (9th Cir. 2011). Cafasso believed that her employer was defrauding the U.S. government by neglecting to protect the government's interest in patents on inventions developed under federal contracts. 2009 WL 1457036 at *2. She reported her concerns in vague terms to company officials, and soon received notice of her termination as the result of what the court found to be a coincidental, non-retaliatory reorganization of her entire work group. *Id.* at *3-4. Apparently concerned that the reorganization might lead to the disappearance of evidence of the fraud she suspected, Cafasso then proceeded to download more than ten gigabytes (21 CDs) of her employer's data, including trade secrets belonging to the employer and third parties, proprietary research and development information, over 30,000 emails, and one patent application with sensitive national-security implications. *Id.* at *5-6. In her sweep of the employer's computer data, the court found, Cafasso did not stop to review individual files to determine their relevance to the fraud she believed was occurring, but instead vacuumed up as much information as she could on her way out the door. *Id*. at *6. The employer eventually discovered Cafasso's actions and demanded the return of its information, but Cafasso refused. *Id.*

The employer filed suit against Cafasso for breach of a confidentiality and non-disclosure agreement that Cafasso had signed, misappropriation of trade secrets, and conversion. *Id.* at *8. Ten days later, Cafasso brought a *qui tam* action along with a claim for retaliation under the FCA. *Id.* After dismissing Cafasso's *qui tam* claims for failure to state a claim and granting summary judgment to the employer on her retaliation claim, the court granted the employer's motion for summary judgment on its claim for breach of contract. The court rejected Cafasso's contention that the FCA, under the circumstances described above, protected her gathering of documents in her investigation of a potential *qui tam* claim. The court explained:

> Public policy does not immunize Cafasso. Cafasso confuses protecting whistleblowers from retaliation for lawfully reporting fraud with immunizing whistleblowers from wrongful acts made in the course of looking for fraud[.] Statutory incentives encouraging investigation of possible fraud under the FCA do not establish a public policy in favor of violating an employer's contractual confidentiality and nondisclosure rights by wholesale copying of files admittedly containing confidential, proprietary, and trade secret information.

Id. at *14.[7]

The Court of Appeals upheld the district court's decision. *Cafasso, U.S. ex rel. v. General Dynamics C4 Sys., Inc.*, 637 F.3d 1047. It noted, "Although we see some merit in the public policy exception that Cafasso proposes, we need not decide whether to adopt it here. Even were we to adopt such an exception, it would not cover Cafasso's conduct given her vast and indiscriminate appropriation of GDC4S files." *Id.* at 1062. The employer later sought over $2,000,000 in sanctions and attorneys' fees from Cafasso and her counsel. *See U.S. ex rel. Cafasso v. General Dynamics C4 Systems, Inc.*, No. CV06-1381, 2009 WL 3723087, at *1 (D. Ariz. Nov. 3, 2009) (employer secured award of $300,000 in attorneys' fees from plaintiff).

The Department of Justice has defended whistleblowers who face counterclaims in *qui tam* cases for having taken employer data for use in their lawsuits, including in the *Grandeau* and *Head* cases discussed above. In *Grandeau*, the Department of Justice filed an *amicus* brief in support of the relator's motion to dismiss the employer's counterclaims. *See* Brief of United States as Amicus Curiae Supporting Relator's Motion to Dismiss the Counterclaims of Defendant, *United States ex rel. Jackie Grandeau v. Cancer Treatment Ctrs of America, et al.*, Case No. 99 C 8287 (E.D. Ill. Apr. 2, 2004) (Docket No 100). In *Head*, the government filed its

[7] *See also Zahodnick v. IBM Corp.*, 135 F.3d 911, 915 (4th Cir. 1997) (rejecting FCA retaliation claim filed after employee realized his voluntary resignation rendered him ineligible for enhanced severance package, and upholding employer counterclaim for violating non-disclosure agreement by sending confidential documents to counsel).

own motion to dismiss. *See* Motion to Strike Affirmative Defense and to Dismiss Counterclaims and supporting brief, *United States ex rel. Head v. The Kane Company, et al.*, No. 05-00317 (D.D.C. Aug. 27, 2009) (Docket Nos. 60, 63).

2. Sarbanes-Oxley Act Retaliation

In at least some cases, evidence-gathering is protected activity in retaliation cases under the Sarbanes-Oxley Act, 18 U.S.C. § 1514A.[8] In a 2011 decision by the Administrative Review Board of the United States Department of Labor, *Vannoy v. Celanese Corp.*, 2008-SOX-00064, ARB No. 09-118, 2011 WL 4690624 (ARB Sept. 28, 2011), the complainant took personnel information from his employer's files as evidentiary support for a tip he had filed with the IRS Whistleblower program alleging that the company had engaged in tax fraud. The ARB found as follows:

> In this case, Vannoy was sharing information with the IRS; information that he believed revealed not only violations of tax laws but also violations that that fell within SOX's reach. There is nothing in the statutory language that limits the agencies to which a complainant may report information in furtherance of enforcement of laws that fall within the SOX's coverage. Vannoy reported the alleged misconduct to individuals who had the authority to investigate the misconduct. It would be incompatible with the congressional intent to promote disclosures of corporate misconduct to narrowly construe the statute in such a way that only reports to the SEC warrant its protection.

Id. at *10.

The ARB in *Vannoy* based its finding of protected activity on the fact that the complainant was reporting not only potential tax laws but also violations "that fell within SOX's reach." *Id.* at *10, but ultimately remanded the case to an ALJ for a determination regarding the

[8] *See, e.g.*, *JDS Uniphase Corp. v. Jennings*, 473 F. Supp. 2d 698, 704 (E.D. Va. 2007) (Sarbanes-Oxley retaliation); *Dartey v. Zack Co. of Chicago*, 1982-ERA-2 (Sec'y Apr. 25, 1983) (nuclear whistleblower under the Energy Reorganization Act, whose anti-retaliation provisions are very similar to those found in SOX Section 806) (http://www.oalj.dol.gov/PUBLIC/WHISTLEBLOWER/DECISIONS/ARB_DECISIONS/ERA/82ERA02C.HTM).

circumstances surrounding the complainant's procurement of the information and his purpose in procuring it, *id.* at * 12. On remand, the ALJ recently ruled in favor of the complainant, finding that the circumstances were appropriate and that the complainant had neither secured the documents in a nefarious way nor shared them with inappropriate parties. *Vannoy v.Celanese Corp.*, 2008-SOX-00064 (ALJ Jul. 24, 2013).

It does not follow from the *Vannoy* decision that any employee who takes documents from an employer and gives them to a regulatory or law-enforcement agency has engaged in protected activity. However, SOX's reach today is very broad, as the ARB in recent cases has found protected activity where the complainants reported a wide range of fraudulent activity.[9] In this context, the *Vannoy* decision sends a strong signal that that the appellate body hearing the largest number of whistleblower cases arising under federal statutes will support employees who take reasonable steps to provide regulators with evidence of unlawful conduct.

3. Dodd-Frank Whistleblower Protections

In promulgating its rules for the securities whistleblower program it administers under the Dodd-Frank Act, the SEC took seriously the new law's goal of incentivizing individuals to provide useful information to the commission. In order to qualify for a reward under the SEC whistleblower reward program Dodd Frank created, a whistleblower must "voluntarily provide" the SEC with information concerning a securities violation and that information must be "original information" – in general, information that is not publicly available, not privileged, and

[9] *See, e.g., Sylvester v. Parexel Int'l LLC*, ARB No. 07-123, ALJ Nos. 2007-SOX-039 (ARB May 23, 2011) (falsifying clinical-trial data in reports to FDA); *Funke v. Federal Express Corp.*, ARB No. 09-004, ALJ No. 2007-SOX-043 (ARB July 8, 2011) (mail fraud by employer's customer); *Inman v. Fannie Mae*, ARB No. 08-060, ALJ No. 2007-SOX-047 (ARB June 28, 2011) (accounting errors already known to employer).

not already known to the SEC.[10] The Dodd-Frank Act also creates a new cause of action whistleblowers who face retaliation by their employers for providing information about securities violations to the SEC, or who initiate, testify, or assist in any SEC investigation, or make disclosures "required or protected" under various laws and regulations.[11]

The statutory protections themselves suggest that employees who provide "purloined" documents to the SEC may be engaging in protected activity under the Dodd-Frank Act, but an SEC rule implementing the whistleblower program makes the protection explicit. Final Rule 21F-17(a) reads, "No person may take any action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement … with respect to such communications." 17 C.F.R. § 240.21(F)-17(a). This prohibition, which has no parallel in the FCA context or in the regulations governing the IRS whistleblower program, can be read to apply both to blanket confidentiality agreements that all company employees sign and to the confidentiality provision that a former employee signs when negotiating a separation from the company. Representatives of the SEC Office of the Whistleblower have made very clear in discussions with lawyers who represent whistleblowers, including the authors, and with lawyers representing corporations, that they intend to enforce this provision aggressively.[12]

---

[10] 17 C.F.R. § 240.21f-4(b)(1).

[11] 15 U.S.C. § 78u-6(h)(1); 17 C.F.R. §240.21F-2(b).

[12] For a comprehensive explanation of the impact of this and related SEC regulations on the protected nature of employees' communications with the SEC, *see* David J. Marshall and Debra S. Katz, A Letter to SEC Commissioners re: The Use of Severance Agreements to Impede Individuals from Participating in the SEC Whistleblower Program: A Growing Problem and a Recommendation (May 8, 2013), at http://kmblegal.com/wordpress/wp-content/uploads/130508-Letter-to-SEC-Commissioners.pdf

C. Framing the Procurement of Confidential Documents as Protected Activity

As these cases illustrate, it is not easy – but likewise not impossible – to convince a court or regulator that a whistleblower who has acquired and disseminated "confidential" documents to appropriate authorities has engaged in protected activity. Framing the whistleblower's actions correctly by emphasizing key facts is crucial. It helps to be able to show that the whistleblower "innocently" came across the confidential document in the course of her work, such as by being copied (even if inadvertently) on an internal memorandum, or by discovering a document mistakenly left on the copier.[13] If the employee did not come across the documents "innocently" but instead searched for them, her lawyer should attempt to present evidence that the employer, upon learning of the employee's protected activity, would likely have destroyed the evidence before the whistleblower would gain access to it through more accepted means such as civil discovery. For example, evidence that the employer has not complied with discovery rules in the past, or has withheld relevant documents requested by regulators, could shift the balance towards the whistleblower's need to collect evidence to support her claims.[14]

If the employee is still employed and the employer discovers the employee's access of and dissemination of documents, the employee should take care not to be insubordinate or give any false explanation when questioned about the matter. The employee's counsel may be able to negotiate a result where the employee does not have to answer the questions in the first place, and refusing to answer may itself constitute protected activity in some contexts. This may be

[13] The *Kempcke* court specifically cites these two scenarios as examples of how an employee might "innocently" acquire a document. 132 F.3d at 446.

[14] *Cf. O'Day*, 79 F.3d at 763 (holding that plaintiff's actions were not protected even though defendant had a history of destroying documents because plaintiff disseminated the documents to a coworker and had preserved documents that did not relate to his specific grievance).

particularly true in a *qui tam* case where the employee is a cooperating government witness and answering might disclose the existence of the sealed case and jeopardize the government's investigation, or in connection with an SEC tip, where an employer's questions about whether the employee has shared information with any agency might be designed to "impede" the employee in further communications with the commission. In general, however, an employee risks termination for refusing to disclose to the employer how he obtained confidential information and what he did with it. Finally, it is important that the whistleblower avoid disseminating the documents to anyone other than her lawyers and appropriate authorities.[15]

II. Acquisition and Dissemination of Documents as Pretext for Retaliation.

Even if a whistleblower or a victim of discrimination fails to convince a court that her acquisition and dissemination of confidential documents were protected activities, she may still be able to keep her retaliation claim alive if the employer used those actions as pretexts to retaliate against her for other protected activities, such as reporting misconduct to regulators or law enforcement. In *Quinlan v. Curtiss-Wright Corporation*, for example, the court upheld a jury verdict for the plaintiff where the jury determined that the plaintiff was the victim of retaliatory discharge. The jury found that the defendant employer's proffered reason for action was pretextual and that it had fired the plaintiff because she brought a case of discrimination against the defendant, not because she had engaged in theft and breached company policies by giving company documents to her lawyers. 8 A.3d at 229. In doing so, the New Jersey Supreme Court determined that while the taking of the documents itself was not a protected activity given

[15] As a practical matter, of course, an employer may be very reluctant to take action against an employee for sharing documents with government agencies. When an employer punishes an employee for doing so, regulators and the public might conclude that the employer is determined to thwart the regulators – and thus the public – in effective regulation of the industry. In fact, the SEC regulations implementing the Dodd Frank Act, discussed *supra*, expressly prohibit employers from preventing employees from bringing certain information to the SEC. 17 C.F.R. § 240.21F-17(a).

the case facts, the employer could nonetheless be held liable for terminating the employee where the employer uses the fact that the employee took documents as a way to disguise what was instead a retaliatory adverse action.

Under the burden-shifting analysis employed by the New Jersey Supreme Court and applied under Title VII and some whistleblower laws, if an employee makes a *prima facie*[16] showing that her protected activity motivated the employer's decision to take an adverse employment action, the employer may rebut the showing by producing evidence that the adverse action was motivated by a legitimate non-retaliatory reason.[17] Once the employer meets this burden, the burden then shifts to the employee to establish that the reason proffered by the employer was pretextual.[18]

In the case of a whistleblower who has wrongfully acquired and disseminated documents, an employer is likely to assert that the non-retaliatory reason for the adverse employment action was the employee's misappropriation of confidential documents, not the fact that she made protected disclosures. An employee in this position is not doomed, however, if she can show enough evidence that the employer's legitimate non-retaliatory reason is pretextual, she can still prevail.[19]

Other whistleblower laws, including the anti-retaliation provisions of the Energy Reorganization Act and the Sarbanes-Oxley Act, do not apply the *McDonnell Douglas* burden-shifting framework, and instead use a framework more akin to the mixed-motive framework used

[16] A *prima facie* showing for many whistleblower causes of action requires the following elements: (1) the employee engaged in protected activity, (2) the employee suffered adverse action, and (3) there is an inference of causation between the protected activity and the adverse action. *Bechtel Const. Co. v. Secretary of Labor*, 50 F.3d 926, 933-34 (11th Cir. 1995); *see also McDonnell Douglas Corp. v. Green*, 411 U.S. 792, 802 (1973).

[17] *See St. Mary's Honor Center v. Hicks*, 509 U.S. 502, 509 (1993).

[18] *Id.*

[19] *Id.*

in discrimination cases.[20] Under these laws, the employee must prove by a preponderance of the evidence only that his protected activity was a "contributing factor" in the employer's decision to take adverse personnel action against him. If the employee makes this showing, the employer can escape liability only if it can demonstrate by clear and convincing evidence that it would have taken the action even in the absence of the protected activity.[21]

One of the more powerful ways of demonstrating pretext (and of rebutting the employer's assertion that it would have taken the action anyway) is to point to a comparator, such as another employee who purloined documents, whom the employer treated more leniently than the whistleblower.[22] Other possible means would be that the employer did not classify the documents at issue as confidential prior to the employee's use of the documents. It should be noted, however, that a retaliation case may turn on whether the employer *believed* that the employee mishandled confidential information, as a good-faith belief may be sufficient to establish a legitimate, non-retaliatory reason for the employer's actions.[23] Of course, any direct evidence, such as statements by the employer that it was firing the whistleblower for protected activity and not for mishandling the documents, would also help establish pretext or rebut the argument that the employer would have taken adverse action even absent protected activity.

---

[20] The U.S. Supreme Court did away with the mixed-motive analysis of retaliation cases under Title VII in *University of Texas Southwestern Med. Ctr. V. Nassar*, No. 12-484, 133 S. Ct. 2517 (2013). While the similar "contributing factor" standard is written into a number of whistleblower-retaliation statutes, the Supreme Court's decision is likely to work against the interests of whistleblowers in areas in which the courts have relied heavily on Title VII jurisprudence for setting standards for proof of causation.

[21] *See Collins v. Beazer Homes USA, Inc.*, 334 F. Supp. 2d 1365, 1376-77 (N.D. Ga. 2004), *citing Stone & Webster Eng'g Corp. v. Herman*, 115 F.3d 1568, 1572 (11th Cir. 1997)).

[22] *See JDS Uniphase Corp.*, 473 F. Supp. 2d at 712 ("[A] properly situated comparator may help establish pretext[.]"); *Clifton v. United Postal Serv.*, 94-STA-0016 (Sec'y May 9, 1995); Dartey, 82-ERA-2, at pg. 7 (Sec'y Apr. 25, 1983) (noting that the complainant could not show that other employees who had engaged in similar conduct were treated more leniently).

[23] *Niswander*, 529 F.3d at 728.

Because courts have been reluctant to find that an employee's use of confidential documents is protected activity, demonstrating pretext (or that the employer would not have disciplined the employer for misuse of confidential information absent her protected activity) is likely to be a whistleblower's best means of protecting her retaliation claim when the employer claims to have taken action against the employee for the purloining of documents.

As a practical matter, of course, an employer may be very reluctant to take action against an employee for sharing documents with government agencies even in the absence of regulations or judicial precedent giving protection to such disclosures. When an employer punishes an employee for providing information to regulators or law enforcement about serious wrongdoing that threatens the public health, safety or economic well-being, regulators and the public might conclude that the employer is determined to thwart the regulators – and thus the public – in effective regulation of the industry.

III. After-Acquired Evidence.

Whistleblowers who have successfully acquired and disseminated confidential documents without their employers' knowledge do not necessarily escape the negative effects of their evidence-collecting methods. If such a whistleblower gets fired for his protected activity and then pursues a retaliation claim against his employer, he may find his remedies limited by application of the after-acquired evidence doctrine.[24] After-acquired evidence is evidence of misconduct for which an employer would have terminated the employee if the employer had known of the misconduct. While after-acquired evidence does not negate liability, it is taken

[24] *See O'Day*, 79 F.3d 756 (after-acquired evidence doctrine applicable where misconduct occurred after plaintiff was informed of adverse employment decision); *Nesselrotte v. Allegheny Energy, Inc.*, 615 F. Supp.2d 397 (W.D. Pa. 2009).

into consideration when determining a plaintiff's remedies.[25] Generally, neither reinstatement nor front pay is considered appropriate in cases where the after-acquired evidence demonstrates that an employer would have terminated the employee for the misconduct if it had been discovered at the time it occurred.[26] Backpay is not barred, but recovery of backpay is usually limited to the time between the unlawful discharge and the date the employer discovers or "acquires" evidence of the employee's wrongdoing.[27]

An attorney representing a whistleblower in litigation should assume that discovery will reveal the employee's appropriation of confidential documents. Because a whistleblower must generally prove as an element of her claim that her belief that the employer was engaging in misconduct was a reasonable one,[28] the factual basis for her belief is relevant in the retaliation action, and her acquisition and handling of any confidential documents that informed her belief is thus open to discovery. A whistleblower who receives an early settlement offer should thus give serious consideration to the likely effects of discovery and the after-acquired evidence doctrine when weighing the relative benefits of settlement and further litigation. Where a significant amount of time will have passed between the retaliation and the discovery of the adverse information, it may be worth continuing to pursue the retaliation action because the recoverable back pay will be substantial even when limited by after-acquired evidence. However, many whistleblower actions, particularly those adjudicated in an administrative

[25] *McKennon v. Nashville Banner Pub. Co.*, 513 U.S. 352 (1995).

[26] *Id.* at 361; *see, e.g.*, *Smith v. Tennessee Valley Authority*, 89-ERA-12, at p. 3 (Sec'y Mar. 17, 1995) (holding that *McKennon v. Nashville Banner Pub. Co.* applied in the context of a whistleblower retaliation suit under the Energy Reorganization Act).

[27] *McKennon*, 513 U.S. at 362.

[28] *Welch v. Chao*, 536 F.3d 269 (4th Cir. 2008), *cert. denied* 129 S. Ct. 1985 (2009).

forum,[29] proceed quickly and thus allow only a limited time for backpay accrual before being cut off by after-acquired evidence uncovered through discovery.

When anticipating an after-acquired evidence problem, the whistleblower and his attorney should also consider whether they can defeat the employer's assertion that it would have terminated the whistleblower if it had known he was purloining confidential documents. The after-acquired evidence doctrine rests on the belief that anti-discrimination laws should not work to abrogate an employer's prerogative to terminate an employee for engaging in misconduct.[30] In order to benefit from the doctrine, the employer has to prove by a preponderance of the evidence that it would have terminated the employee for the misconduct upon discovering it.[31] Evidence that the employer has not terminated other employees for similar transgressions would serve to refute the employer's assertion that it would have terminated the whistleblower for her actions if it had known about them.[32] A whistleblower might also be able to obtain information through discovery demonstrating that the documents were not actually confidential, or treated by the employer as such, so that she did not actually engage in misconduct by acquiring and disseminating them.[33]

IV. Employee's Potential Civil Liability for Taking Employer Documents.

[29] *See, e.g.*, Clean Air Act, 42 U.S.C. § 7622 (2006) (30-day statute of limitations); Federal Water Pollution Control Act, 33 U.S.C. § 1367 (2006) (30-day statute of limitations); Solid Waste Disposal Act, 42 U.S.C. §6971 (2006); Toxic Substance Control Act, 15 U.S.C. §2622 (2006); Wendell H. Ford Aviation Investment and Reform Act for the 21st Century ("AIR 21") 49 US.C. § 42121 (West 2008) (90-day statute of limitations).

[30] *McKennon*, 513 U.S. at 362.

[31] *O'Day*, 79 F.3d at 761.

[32] *Nesselrotte*, 615 F.Supp.2d 397, at 405-06 (although the plaintiff is unsuccessful because she failed to provide sufficient evidence to create a genuine issue of fact, the court considered plaintiff's argument that defendant would not have fired her for her misconduct).

[33] *Id.* at *5 (plaintiff unsuccessfully argued that employer had consented to her use of the confidential documents).

Some whistleblowers face a greater risk than mere weakening of their retaliation cases if they wrongfully acquire and disseminate confidential documents. Employers in recent years have begun to bring civil claims against employees who blow the whistle using confidential documents, and some whistleblowers have even faced criminal prosecution for their use of confidential documents. Since a whistleblower may be opening herself up to significant civil and criminal liability, it is important to be able to advise the whistleblower of the possible claims an employer might bring and the level of exposure that the whistleblower has to civil and criminal penalties before moving forward with a whistleblower action . A consult with a criminal attorney may be advisable as well in some cases. Some of the possible bases for employee liability are discussed below.

A. Breach of Contract Requiring Confidentiality

Employers increasingly require employees to sign confidentiality agreements that limit their use of confidential or proprietary information during and after their employment. This is most often the case for employees who have access to trade secrets and other proprietary or confidential information in the course of their work. While confidentiality agreements vary in their breadth and scope, most such agreements prohibit the employee's disclosure of confidential or proprietary information to anyone outside the company without prior permission from the company, and require the employee to return all such information upon termination of her employment. A whistleblower who has signed this type of confidentiality agreement may be liable for breach of contract if she disseminates confidential information in the process of blowing the whistle because she would presumably be disclosing the information without company approval. She may also face liability if the employer has already terminated her and

she has failed to return all confidential and proprietary information in her possession as required by the agreement.

Even in the absence of case law or regulation making their actions "protected activity," some whistleblowers have successfully defended such breach-of-contract suits by arguing that the confidentiality agreements were unenforceable on public-policy grounds, citing the public policy in favor of effective reporting of misconduct that harms the public interest.[34] It is a well-established principle of contract law that a promise is unenforceable if, under the circumstances, the interest in its enforcement is outweighed by a public policy that would be undermined by its enforcement.[35] Although some courts have acknowledged that a confidentiality agreement might be unenforceable on such public-policy grounds,[36] other courts have enforced confidentiality agreements in spite of the same arguments where an employee has disseminated confidential documents in violation of the contract.[37] As discussed *supra*, the SEC regulation prohibits enforcement of confidentiality agreements if such agreements would prevent employees from bringing information to the attention of the SEC.[38]

Based upon the reasoning of courts that have considered this issue, it is likely that a court will declare a confidentiality agreement unenforceable on public-policy grounds only if the court

[34] *JDS Uniphase Corp.*, 473 F. Supp. 2d 697; *Saini v. Int'l Game Tech.*, 434 F. Supp. 2d 913, 923 (D. Nev. 2006).

[35] *Town of Newton v. Rumery*, 480 U.S. 386, 392 (1987); *see also* RESTATEMENT (SECOND) OF CONTRACTS § 178 (1981).

[36] *Saini*, 434 F. Supp. 2d at 923 (Court identified three different situations where a confidentiality agreement might not be enforceable: "(1) if the interests in the agreement's enforcement is outweighed in the circumstances by a public policy harmed by enforcement of the agreement, (2) if the agreement is being used by one party within the context of litigation to suppress an adverse party's access to evidence, and (3) if the employee is disclosing an illegal or wrongful act for a purely public purpose, such as whistleblowing.").

[37] *JDS Uniphase Corp.*, 473 F. Supp. 2d 697; *Saini*, 434 F. Supp. 2d at 923 (holding that the public's interest in uncovering any sale of defective gambling devices that did not threaten the safety or economic well-being of the public at large was not sufficiently great to outweigh the public interest in enforcement of trade secret and confidentiality agreements).

[38] 17 C.F.R. § 240.41f-17(a).

determines that the public policy is sufficiently "well defined and dominant,"[39] and also that, in the particular case, the policy outweighs the interest of the employer in enforcing the agreement and protecting its confidential information. For example, in *JDS Uniphase Corporation v. Jennings*, the plaintiff argued that a confidentiality agreement was unenforceable because the California legislature had proclaimed it a public policy of the state to:

> Encourage employees to notify an appropriate government or law enforcement agency when they have reason to believe their employer is violating laws enacted for the protection of corporate shareholders, investors, employees, and the general public.

473 F. Supp. 2d at 701. Despite this declaration of public policy in favor of whistleblowing, the court held the confidentiality agreement enforceable because the public policy was too generalized, did not address the enforceability of confidentiality agreements, and did not make it clear that otherwise unlawful or tortious activity was excused or permitted as long as it arguably aided whistleblowing activity. *Id.* at 702. The *Jennings* court explained that, even if there had been a valid public policy allowing employees to pilfer their employers' confidential documents to prove misconduct, its effect would be outweighed in practice by its propensity to encourage disgruntled employees to steal confidential documents when those documents were available by other means, such as civil discovery. *Id*. at 702-03.

An additional exception would likely be the reporting of major criminal activity, especially activity that might cause bodily harm.[40] While there is no case law directly on point, the criminal codes of all jurisdictions provide well-defined policy grounds against major criminal

[39] *W.R. Grace and Co. v. Local Union 759*, 461 U.S. 757, 766 (1983).

[40] *See* Richard A. Lord, 7 WILLISTON ON CONTRACTS §15:8 (4th ed. 2008) ("The better rule is that all bargains tending to stifle criminal prosecution, whether by suppressing investigation of crime or by deterring citizens from their public duty of assisting in the detection or punishment of crime, are void as against public policy.").

activity. If a whistleblower can show that her disclosures pointed specifically to such activity, it is likely that she could convince a court that the public's interest in stopping and deterring major criminal activity outweighs her employer's interest in maintaining the confidentiality of documents.

B. Breach of Fiduciary Duty

Under general principles of agency law, an employee has a duty not to use or communicate information confidentially given to her by the employer, or acquired by her during the course of or on account of her employment, unless the information is a matter of general knowledge.[41] However, an employee as agent may reveal confidential information acquired in the course of her employment if she is acting to protect a significant public interest, such as reporting the fact that the employer is committing or is about to commit a crime.[42]

As with breach-of-contract claims, the few reported decisions addressing this issue indicate that courts are reluctant to exempt employees' dissemination of confidential information for whistleblower purposes from the constraints of their fiduciary duties to their employers. In *Nesselrotte v. Allegheny Energy, Inc.*, 615 F. Supp.2d 397, 410 (W.D. Pa. 2009), the court held that the plaintiff, former in-house counsel for the defendant, violated her fiduciary duty to her former employer (and client) by retaining confidential information for use as evidence in an age discrimination lawsuit. In *Bordell v. General Electric Co.*, 556 N.Y.S. 2d 234, 235 (N.Y. Sup. Ct. 1990), the court went as far as to find that an employer could state a claim for breach of fiduciary duty where the employee, among other acts of misconduct, had disclosed confidential

[41] RESTATEMENT (SECOND) OF AGENCY § 395 (1958).

[42] *Id.*; *see also Caesar Elecs. Inc. v. Andrews*, 905 F.2d 287, 289 (9th Cir. 1990) ("However high the duty an agent may owe its principal, society's interest in preventing the commission of criminal acts overrides that duty, as exemplified by the wealth of state and federal criminal conspiracy statutes in this county.").

information while blowing the whistle on a serious issue of public health and safety – radiation overexposure.

C. Counterclaims as a Form of Retaliation

The specter of being sued for breach of fiduciary duty or breach of contract, on top of getting fired, is enough to dissuade many potential whistleblowers from coming forward to report employer wrongdoing. Courts have acknowledged that such suits, if in bad faith, can be the grounds for an additional retaliation claim by a whistleblower because a reasonable employee who faces the choice of avoiding an employer's countersuit (even if groundless) and pressing ahead with a discrimination or retaliation claim (even if valid) might chose the former.[43] To successfully plead a retaliation claim based on an employer's filing suit against the employee, the whistleblower must show that the employer's suit is brought in bad faith and that there is a causal connection between the employer's counterclaim and the whistleblower's protected activity or original legal action.[44] Whistleblowers who have acquired and disseminated confidential documents may find it difficult to meet this standard because, as reflected in some of the cases cited above, the purloining of documents may provide the employer with the necessary legal and factual basis for a non-retaliatory counterclaim. For example, in *U.S. ex rel Head v. Kane Co.*, discussed *supra*, the court dismissed counterclaims against the relator by the former

[43] *Nesselrotte v. Allegheny Energy, Inc.*, No. 06-01390, 2009 WL 703395, *14 (Mar. 16, 2009) (holding that counterclaims of breach of contract and breach of fiduciary duty could constitute adverse action under *Burlington Northern* standard); *see also Bill Johnson's Rests.*, 461 U.S. 731, 743-44 (employer's lawsuit against employees for assertion of labor rights constituted retaliation under the NLRA); *Darveau v. Detecon, Inc.*, 515 F.3d 334 (4th Cir. 2008) (holding that plaintiff had a claim for retaliation despite the court rejecting the employee's underlying FLSA claim); *Hernandez v. Data Sys. Int'l, Inc.*, 266 F. Supp. 2d 1285, 1306 (D. Kan. 2003) ("[R]etaliatory civil litigation can constitute an adverse employment action for purposes of a retaliation claim.").

[44] *Darveau*, 515 F.3d 334 (finding that plaintiff's employer's filing of a lawsuit against him alleging fraud was an adverse action because the employer had a retaliatory motive and did not have a reasonable basis in fact or law for the suit.); *Nesselrotte*, 2009 WL 703395 at *14 (holding that the plaintiff failed to establish a causal connection between her discrimination filing and the defendant's filing of counterclaims and that the defendant's claims that the plaintiff violated her fiduciary duty and breached her confidentiality agreement were not frivolous).

employer for having taken documents and provided them to the government as part of the relator's disclosure under the False Claims Act.

V. Criminal Liability.

Although few whistleblowers have incurred criminal liability for acquiring and disseminating confidential documents without their employers' permission, several recent examples suggest that prosecution of employees and former employees on such grounds is a risk that warrants attention from lawyers representing whistleblowers.[45] The following recent examples give whistleblowers and their lawyers reason for serious concern:

- In 2008, Boeing employee Gerald Eastman blew the whistle on alleged quality assurance and inspection problems by leaking documents to newspapers. As a result of his actions, Eastman was tried for felony computer trespass in April 2008, resulting in a hung jury.[46] King County prosecutors, after significant urging from Boeing, initially indicated that they would try Mr. Eastman a second time. In order to avoid a second criminal trial and potentially 3.5 to 4.5 years in jail,[47] Eastman settled with the government by promising to help recover the documents he had leaked and to cooperate in any legal proceedings that arose from the company's efforts to retrieve the documents.[48]

- Two nurses in Texas faced trial on felony charges for supposed "misuse of official information" in their reporting of patient-care issues to the state medical board. The nurses, who had each worked at Winkler County Memorial Hospital for ten or more years, filed an anonymous complaint with the board reporting that a doctor at the facility was operating a side business selling sham herbal remedies to patients. Authorities searched the nurses' computers, found their complaint, and indicted them on third-degree felony charges.[49] Although prosecutors dismissed charges against one of the nurses and a jury acquitted the other after deliberating for only one hour, their experience with the law cannot but have a chilling effect on medical

[45] Employees who "purloin" documents may face criminal liability for theft of trade secrets or under other statutes, including the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; National Stolen Property Act, 18 U.S.C. § 2314, and the Electronic Espionage Act, 18 U.S.C. § 1831.

[46] Natalie Singer, *Was Inspector Source of Leak at Boeing?*, THE SEATTLE TIMES, Mar. 26, 2008, *available at* http://seattletimes.nwsource.com/html/boeingaerospace/2004306499_leaktrial26m.html.

[47] *Id*.

[48] Mike Carter and Steve Miletch, *Whistle-blower Settles Case*, THE SEATTLE TIMES (July 11, 2008) available at: http://seattletimes.nwsource.com/html/localnews/2008046014_eastman11m0.html.

[49] *See* http://junkfoodscience.blogspot.com/2009/09/who-will-speak-out-for-you.html.

professionals.[50] But the story ended well: the nurses later sued the county and county officials, won a $750,000 settlement, and no doubt found additional solace in the board discipline of the doctor and the criminal convictions and jailing of the sheriff and county attorney who led the campaign of retaliation.[51]

- The IRS whistleblower who reported unlawful tax sheltering by UBS and saved the government nearly a billion dollars was sentenced to prison for his role in the wrongdoing. While it is true that ex-banker Bradley Birkenfeld was complicit in creating unlawful tax shelters for clients, it was only because of his about-face and cooperation with the IRS that taxpayers were able to recoup lost taxes, and the IRS was able to put UBS out of the tax shelter business.[52] In fact, the IRS announced in September 2012 that it approved an award of $104 million to Mr. Birkenfeld. Birkenfeld's case is not about the collection and dissemination of documents, but it demonstrates that stepping forward and blowing the whistle on wrongdoing is no guarantee that prosecutors will forgive related wrongdoing on the whistleblower's part. [53]

Most prosecutors appear unwilling to pursue criminal charges against whistleblowers, but attorneys representing whistleblowers should not ignore the possibility that their clients could become exposed to criminal liability by sharing confidential documents that they acquire from their employers. The risk is greater where, as in the Boeing case described above, the employee has accessed the information through the employer's computer system, as unauthorized computer access may violate a number of recent criminal statutes, such as computer trespass and unlawful computer access, that were originally target computer hackers who attacked systems but can be used to prosecute whistleblowers as well.[54]

The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*, was designed primarily for the criminal prosecution of computer hackers for "unauthorized" accessing of and causing

[50] http://www.nytimes.com/2010/02/12/us/12nurses.html.
[51] http://seattletimes.com/html/nationworld/2016396245_apusnursesretaliation.html
[52] *See* http://www.time.com/time/business/article/0,8599,1928897,00.html.
[53] Stephen Heller was charged in Los Angeles Superior Court with felony access to computer data, commercial burglary, and receiving stolen property for releasing confidential information regarding Diebold's certification of voting systems. Hemmy So, *Man Pleads Not Guilty in Voting Device Case*, LOS ANGELES TIMES, (Feb. 22, 2006), *available at* http://articles.latimes.com/2006/feb/22/local/me-diebold22.
[54] *See* Singer, *supra* note 51; *see also* Nikola Strahija, *Wi-Fi Whistle Blower Faces Criminal Charges*, Xatrix Security (Sep. 17, 2003), *available at* http://www.xatrix.org/print.php?s=3551.

harm to computers used in interstate commerce, but the law also has a civil-action provision. The CFAA prohibits several types of accessing of computers "without authorization or exceeding authorized access."[55] What constitutes "authorization" for access is not settled and is the subject of a split among the circuits. The Fifth, Seventh, and Eleventh circuits have adopted a broad interpretation – i.e., that an employee acts without authorization, or exceeds authorization, as soon as the employee acquires an interest adverse to the employer or breaches a duty of loyalty to the employer.[56] The Ninth and Fourth circuits have adopted much narrower readings, as have district courts within the Second Circuit. These courts have held that later misappropriation of the information does not strip the accessing employee of "authorization" as long as the employee was authorized at the time of access.

In *U.S. v. Nosal*, 676 F.3d 854, 856-57 (9th Cir. 2012), an *en banc* Ninth Circuit held that a former employee did not exceed his authorized access under the CFAA when he obtained computerized information from current employees and then used that information for an unauthorized purpose. Nosal left his job at an executive search firm, Korn/Ferry, and, although he had signed a non-competition agreement, nevertheless had former colleagues – who still worked for Korn/Ferry – download and send him information from a confidential database. They had authorized access to the database, but company policy prohibited disclosing the confidential information outside the company. Nosal then used the information to start a competing company. *Id.* at 856.

Nosal was indicted for aiding and abetting his former colleagues in the crime of "exceed[ing] authorized access" for a fraudulent purpose. The district court dismissed the CFAA

[55] 18 U.S.C. § 1030(a).

[56] *See* United *States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), cert. denied 131 S.Ct. 2166 (2011); *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006).

counts, holding that simply using the information for an unauthorized purpose did not constitute exceeding authorized access. *Id.* at 856-57. A Ninth Circuit panel reversed and the *en banc* Ninth Circuit then affirmed the judgment of the district court. *Id.* at 864. The Justice Department declined to seek review of the *en banc* opinion. The court's *en banc* decision in *Nosal* goes further than a previous decision, *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009), in which the Ninth Circuit had rejected the appeal of an employer who argued that a current employee's download of employer data rendered the employee's access "unauthorized" merely because the employee acted for his own benefit and against the interests of the employer.

The Fourth Circuit has joined the Ninth Circuit in rejecting the Seventh Circuit's approach. In *WEC Carolina Energy Solutions, LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012), the Fourth Circuit held that the employer failed to state a claim under the CFAA against a former employee and his assistant[57] where the two employees had allegedly downloaded proprietary information before leaving the company and had later used the information to aid a competitor for whom they had begun working.

The court held that the employees' access – which was authorized at the time they took the confidential information – did not become "unauthorized" merely by virtue of the fact that they misappropriated the information after leaving the company. *Id.*at 206-07. The Supreme Court denied the company's petition for certiorari, leaving the circuit split wide open.[58]

[57] As well as a competitor, although for the purposes of this paper we are concerned only with the employee parties.

[58] *WEC Carolina Energy Solutions, LLC v. Miller*, No. 12-518, R46-006, 2013 WL 28079 (U.S. Jan. 2, 2013).

In *United States v. Aleynikov*,[59] a high-profile case involving the alleged theft of source code used high-frequency trading, the district court dismissed criminal charges against Aleynikov under the CFAA on the grounds he had been authorized to access company computers and did not exceed the scope of his authorization, and that his authorized use of a computer was not a criminal offense under the CFAA even though he used the information in a manner that constituted misappropriation. .[60]

VI. Ethics Issues for an Attorney Whose Client has Purloined Documents.

An attorney whose client presents her with purloined documents is confronted with an array of ethical issues. Can the attorney ethically read the confidential documents? Does the attorney have to return purloined documents to the employer? If the attorney does have to return them, does she have to disclose how she came into possession of the documents and risk exposing her client? The specific ethical obligations of an attorney will depend on the rules of the jurisdiction in which the attorney practices. The following discussion does not address these differences, but rather identifies some important ethical issues that may arise and require further consideration by an attorney whose client possesses purloined documents.

While many of these ethics issues are murky, authorities are in relative agreement that an attorney has an ethical obligation to not participate herself or further the criminal activity, fraud, or deceit of her client or a third party.[61] A particularly egregious example of an attorney's unethical use of purloined documents took place during the litigation of *Lipin v. Bender*. 84 N.Y.2d 564 (1994). During a deposition, the plaintiff took a large pile of legal documents

[59] 737 F. Supp.2d 173 (S.D.N.Y. 2010), reversed on other grounds, *United States v. Aleynikov*, 676 F.3d 71 (2d. Cir. 2012).

[60] *Id.* at 192-94.

[61] *See* MODEL RULES OF PROF'L CONDUCT R. 8.4(b) & (c) (2009); *see also* RESTATEMENT (THIRD) LAW GOVERNING LAWYERS §8 cmt. e (2000).

belonging to the defense from a table, then surreptitiously read through them and made copies. *Id.* at 566-67. When the plaintiff told her attorney, Wisehart, about her actions, Wisehart declined to review the documents himself until he received a "second opinion," but he told the plaintiff to tell defense counsel, if asked, that she had picked the documents up by mistake. *Id.* at 567. The plaintiff refused to agree to lie. *Id.*

The following day, Wisehart approached defense counsel and demanded a settlement in light of a "recent development," *i.e.*, the information contained in the documents the plaintiff had obtained, which allegedly bolstered her case. *Id.* Wisehart refused to tell defense counsel how the plaintiff had obtained the documents, other than to claim that it was legitimate, and said he had no control over plaintiff's use of her own copies of these documents. *Id.* He even suggested that his client might disseminate the documents to the press. *Id.* As might be expected, Wisehart's conduct netted him a two-year suspension from the bar, upheld by the New York Supreme Court, Appellate Division.[62]

While most attorneys would conclude that Wisehart's conduct as a whole rose to the level of unethical, some attorneys may not realize that using a purloined document during settlement negotiations and dodging questions about the source of the document, as Wisehart did, could sufficiently violate the rules against misrepresentation and deceitful conduct to warrant disciplinary action. An attorney also has to be careful when asking her client to search for and copy documents, as doing so could violate ethics rules since searching and removing documents might violate criminal laws.

[62] The court concluded that Wisehart, a member of the bar since 1955, had violated the following disciplinary rules: Disciplinary Rule ("DR") 1-102(A)(4) ("dishonesty, fraud, deceit, or misrepresentation"); DR 1-102(A)(5) ("conduct that is prejudicial to the administration of justice"); DR 1-102(A)(7) ("any other conduct that adversely reflects on the lawyer's fitness as a lawyer); DR 7-106(A) (disregarding or advising client to disregard tribunal's order); and DR 7-106(C)(6) ("engag[ing] in undignified or discourteous conduct which is degrading to a tribunal"). *In re* Wisehart, 721 N.Y.S.2d 356 (N.Y. App. Div. 2001) (*per curiam*).

Jurisdictions are less in agreement on the ethical obligations of an attorney whose client has presented her with purloined documents that are subject to the attorney-client privilege, but who has not participated in or furthered any criminal, fraudulent, or deceitful activity. In the District of Columbia, an attorney who receives materials that are privileged on their face may violate ethical rules by reviewing the materials or by using them in an adversarial hearing, if she had a reasonable basis to conclude that the privilege had not been waived and that the documents had been obtained without authorization.[63] Even if the attorney did not know that the document was privileged at the time of reading, the attorney may still have violated ethical rules if the attorney should have inferred from the circumstances at the time of receipt that the document was privileged.[64] For instance, if the attorney receives a document under suspicious circumstances – *e.g.*, the client says "don't ask me how I got this" – the attorney should insist on clarification before reviewing or using the document.[65]

As long as the privileged status of the document is not apparent on its face, however, and the attorney does not know that the document is privileged when she reads the document, she is probably not in violation of ethics rules in the District of Columbia.[66] Some jurisdictions allow attorneys even more leeway: in Virginia, a lawyer who receives privileged materials unsolicited has no obligation to make a disclosure to a tribunal or to an adverse party, and may review and use such materials.[67]

Given the risk of violating ethics rules and the variations in those rules from state-to-state, an attorney who receives employer documents from a client should proceed with caution.

---

[63] D.C. Bar Legal Ethics Comm., Ethics Op. 318 (2002).
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *See, e.g.*, Virginia State Bar Ethics Comm., Legal Ethics Opinion 1076 (1988).

Look at the documents for indicia of attorney-client privilege, such as an attorney-client disclaimer or the name of in-house counsel, before reading them. Insist that the client disclose fully the circumstances under which he came into possession of the documents. Consult applicable ethics rules and ethics opinions, request an opinion from bar counsel if needed, and retain independent ethics counsel if ethical obligations remain unclear and the case cannot proceed successfully without using the documents in a way that might violate ethics rules.

Even if an attorney has not violated an ethical rule by reading a privileged document, the attorney may still violate ethical rules if she discloses the document without her client's approval. As discussed above, a whistleblower's use of confidential documents can significantly hurt her retaliation case and potentially subject her to civil and criminal liability. Since an attorney must not reveal confidences or secrets that jeopardize a client without first apprising the client of the affects of disclosure and securing the client's permission to make the disclosure,[68] the attorney cannot disclose the document to the opposing party, even for the purposes of seeking settlement, without the client's permission. In some jurisdictions, including the District of Columbia, an attorney's duty of confidentiality would also prevent the attorney from notifying the opposing party and returning a privileged document because that action would likely jeopardize the client's interests.[69]

An attorney's obligations regarding a purloined document that is not privileged, but which the employer claims is confidential or proprietary, are generally less strict than in the case of privileged documents. For example, a whistleblower steals copies of a test report which demonstrates that a nuclear plant has violated federal regulations. The report is not a

[68] *See* MODEL CODE OF PROF'L RESPONSIBILITY DR 4-101 (1980); MODEL RULES OF PROF'L CONDUCT R. 1.6 (2012).

[69] D.C. Bar Legal Ethics Comm., Ethics Op. 242 (1993).

communication between the employer and its attorney or prepared in connection with litigation, but the employer would surely claim that the test report is confidential. In Virginia, an attorney who receives this purloined document would be allowed to use it in her representation of her client, but she would be required to make a copy and return the original.[70] Of course, the attorney's ability to use the document would require the client's agreement for the reasons discussed above. If the client and attorney decide not to return the purloined document, the attorney should still preserve the document since it is the property of a third party.[71]

VII. Advising a Client Who Has Purloined Documents.

As this discussion has surely made clear, the role of purloined documents in a whistleblower case is problematic. Obtaining and using documentation of safety and legal violations can often be the best way for a whistleblower to motivate law enforcement and regulators to investigate her complaint, yet the same actions can undermine her legal case and expose her to civil and criminal violations. In order to maximize the client's protection against such risks, an attorney representing a whistleblower should discourage the whistleblower from wrongfully acquiring documents from the employer. If the whistleblower has seen documentary evidence of wrongdoing, instead of taking or copying the document, she should describe the information in detail to her attorney so that both attorney and client can present her case to the employer, request the documents in discovery, or, if appropriate, report the employer to the appropriate regulators and carefully describe the documentary evidence that they will need to request from the employer in the course of their investigation. If the whistleblower has already taken confidential documents improperly and given them to the attorney, the attorney should

[70] Virginia State Bar Ethics Comm., Legal Ethics Opinion 1141 (1988).
[71] *See* MODEL RULES OF PROF'L CONDUCT R. 1.15 (2012).

consider ways to minimize the harm from the client's actions while still preserving the ability to use the documents in litigation. For example, the attorney might make copies of the documents, Bates-stamp the copies, and return both stacks to the employer while preparing document requests for copies of the numbered documents he has returned. If the client's case involves complaints about securities violations and there are issues at play that should be reported to the SEC, the attorney might advise the client to turn over the documents to the SEC. The attorney might have similar advice for a client whose documents contain evidence of fraud on the U.S. government in violation of the False Claims Act.

Attorneys representing whistleblowers should also keep in mind that, as a practical matter, whistleblowers often use employer documents with impunity because of the nature of whistleblower cases – that is, the employee has stepped forward and risked his job to report unlawful conduct on the part of his employer, conduct which jurors, regulators and even judges might conclude is far worse than the employee's violation of contractual or other duties upon which the employer relies to ensure that its practices will not see the light of day. In these situations, an employer may be very reluctant to take action against an employee who has come into possession of documents that demonstrate the employer's wrongdoing, as "shooting the messenger" can provoke a strong reaction from those that will eventually pass judgment on the employer for its unlawful actions, regardless of what happens to the whistleblower. For this reason, most whistleblower cases that arise from an employee's good-faith allegations of serious wrong on the part of her employer do not result in actions against the employee, even when the employee is in possession of purloined documents.

Employers who would take action against whistleblowers are sometimes deterred as well by the fact that the employer is defending an action in a forum that has no jurisdiction to hear

counterclaims against the employee. For example, the U.S. Department of Labor adjudicates a large number of whistleblower claims arising under nuclear and environmental laws, but the Department cannot hear an employer's claim for breach of contract or breach of fiduciary duty. In order to bring those claims against the employee, the employer must initiate a separate action, often in a state court – a much more public forum than the Department of Labor – whose juries would not look kindly on the activities that the whistleblower has reported, and may look kindly on the employee who has arguably done great benefit to the community at great risk to himself.

The underlying issues in whistleblower cases thus raise the stakes for employers who would sue whistleblowers for using confidential information to expose the employer's wrongdoing, but an attorney who is aware of the risks involved in the use of purloined documents is nonetheless better able to prepare his client's case for success.