"Purloined Letters": Management Options When A Departing Employee Puts A Business Entity At Risk By Collecting Confidential Business Or Personnel Information For Use In The Employee's Personal Litigation

Littler Mendelson, P.C.

Whistleblower/Corporate Ethics Practice Group

Edward T. Ellis – *Philadelphia*
Earl M. Jones, III – *Dallas*
Kevin E. Griffith – *Columbus*
Jill M. Weimer – *Pittsburgh*
Christian A. Angotti – *Pittsburgh*
Bryan M. Gramlich – *Columbus*

Littler®

Table of Contents

The following scenario is more common—and more troubling—than ever before. A high-ranking employee who has signed an agreement to preserve the confidentiality of business plans, financial information, and trade secrets stealthily collects confidential information belonging to the employer. The employee uses a work laptop to access this type of information on the company computer system. This information may be as simple as a few emails, but it may also be strategic business plans, revenue forecasts, new business targets, personnel files, executive deliberations on promotions, legal advice from counsel, records of transactions on a government contract, discount pricing information, or other trade secrets or privileged information. Employees have in some cases gathered such data to use as proof of schemes to defraud shareholders, customers, or the government, or to prove some other unlawful conduct. Oftentimes, however, the purloined information does not prove what the employee thinks it will prove. Sometimes the employee is a lawyer, which raises serious and sometimes complex attorney-client privilege issues for the company, and ethical issues for the lawyer.

The information often leaves the employer's premises attached to an email, or on a hard drive, a USB drive, a disk, or in hard copies in the employee's briefcase or backpack. It may also have been sent electronically to the employee's legal counsel, a government investigator, and/or to a cloud account. The information may contain a treasure trove of competitive business information or information reflecting potentially bad conduct—beyond the employee's initial concerns—that may be of interest to government investigators. Removal of information from an employer's data systems frequently coincides with either the termination of the employee involved or the employee's "unavoidable" resignation under circumstances where the employee will later claim constructive discharge. The employee may claim to be a whistleblower, or may simply be leaving the company to join a competitor or pursue other interests, and subsequently decide months later to also act as a whistleblower against the company.

This scenario puts an employer in a difficult situation. In many cases, top management is not sure whether the employee is simply disgruntled or is on to something legitimate. Thus, a telephone call to law enforcement authorities reporting the theft of valuable intellectual property may not be management's best first move. An internal investigation and initial evidence gathering usually is the preferred first option. In the meantime, the employer's confidential information may be in the hands of a hostile party or subject to public disclosure, and the employer does

not know the parties' intentions. The employer is exposed to anything from a single-plaintiff whistleblower retaliation claim or other wrongful termination or discrimination lawsuit, to a possible criminal investigation, and/or public release of commercially valuable information that could significantly harm its business.

The purpose of this paper is to describe an employer's legal rights and options when an employee has removed confidential information without permission.

I. CAN A BUSINESS ORGANIZATION RETRIEVE AND SECURE THE CONFIDENTIAL INFORMATION TAKEN BY AN EMPLOYEE FOR USE IN AN INVESTIGATION OR SUBSEQUENT LITIGATION?

A. An employer's first reaction to the discovery that its information has been compromised often is to instruct the company lawyers to get it back. This may be easier said than done. Employee confidentiality agreements are of limited value in obtaining retrieval of evidence if the information the employer is trying to protect may be proof of a crime or other unlawful conduct.

Many employers require that employees sign non-disclosure agreements: (1) acknowledging that the company has provided them with confidential and proprietary information, including trade secrets; and (2) promising to preserve the confidentiality of that information. These agreements—often referred to as "NDAs"—are a contractual basis for a lawsuit demanding return of the information. In addition, state statutory and common law has long protected businesses by making theft of trade secrets a civil claim. At the federal level, the Economic Espionage Act (EEA) has made the theft of a company's trade secrets a crime since 1996. The 2016 federal Defend Trade Secrets Act (DTSA), which amended the EEA to provide a federal civil remedy against persons who unlawfully misappropriate an employer's trade secrets, essentially codifies state Uniform Trade Secret Acts and the common law on the theft of trade secrets. But these statutes only protect "trade secrets"—as defined in the EEA—and not all internal business information that an employee might purloin meets this definition.[1] An employer attempting to retrieve and secure confidential information taken by an employee must first determine which of these remedies is available and how the employer can take advantage of them, especially in the face of countervailing public policies that promote whistleblowing.

An initial problem faced by an employer seeking to protect its information is that the courts will generally not allow an employer to keep information secret through a non-disclosure agreement if the information tends to prove that someone in the business committed a crime. This principle is nowhere better illustrated than in *Erhart v. Bofl Holding, Inc.*,[2] which arose under pre-DTSA law. In *Erhart*, the whistleblower—an internal auditor for a federally chartered bank—removed a large volume of highly confidential information, including internal audit reports, audit committee meeting minutes, drafts and back-up information, bank regulators' supervisory information and related communications, lists of customer accounts, specific customer account information, customer Social Security numbers, inquiries from law enforcement and the U.S. Securities and Exchange Commission (SEC) concerning a customer, wire transfer details, and portions of loan files. The district court accepted without lengthy discussion that much of the information qualified as trade secrets and

1 Under 18 U.S.C. § 1839 (3), the EEA defines "trade secret" as "all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—**(A)** the owner thereof has taken reasonable measures to keep such information secret; and **(B)** the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

2 No. 15-CV-02287, 2017 U.S. Dist. LEXIS 20959 (S.D. Cal. Feb. 14, 2017).

that it was a proper subject for a confidentiality agreement. However, the district court also accepted that the information was likely to prove a crime, and that it had been turned over to law enforcement.

The defendant in *Erhart* used the company's information to bring a whistleblower retaliation action invoking the Sarbanes Oxley (SOX) Act and the Dodd-Frank Act, as well as state causes of action. The bank counterclaimed for breach of the confidentiality agreement. The district court addressed the bank's motion for summary adjudication of the affirmative defenses the whistleblower had raised against the bank's counterclaim allegations. The court discussed at length how a California court will not enforce a confidentiality agreement if doing so would violate California public policy, including California's strong policy encouraging whistleblowing and protecting whistleblowers. The court held that the state public policy trumped the enforcement of the non-disclosure agreement, and the court denied the bank's motion to dismiss certain of the whistleblower's affirmative defenses.

Notably, because the whistleblower's actions in *Erhart* preceded the DTSA's enactment of its whistleblower immunity provisions (discussed at length in this paper below), *Erhart* did not address whether the whistleblower's conduct complied with the whistleblower immunity protections in the DTSA. A review of the court's factual summary in *Erhart* shows that the whistleblower's conduct included numerous misappropriations of the bank's trade secret information that would not have warranted immunity protection under the DTSA. Nor did *Erhart* address whether the whistleblower's "self-help" activities—which included electronically transferring large amounts of the bank's electronically stored information to various personal computer equipment and personal email sites, as well as to his mother's computer—violated any other laws, such as the federal Computer Fraud and Abuse Act or state computer use laws.

Thus, in applying only California contract law, the *Erhart* court tried to strike a balance between an employer's right to protect its confidential business data, and a whistleblower's right to expose potentially criminal or other unlawful activity. But, in deciding that California's public policy would not support enforcing the non-disclosure agreement against each one of the whistleblower's acts of misappropriation, the court very much came down on the whistleblower's side of the scales. In doing so, the court carefully assessed in each instance what information the whistleblower took, the manner in which he took it (selectively or indiscriminately), and his proffered reasons for why he took it.

Erhart's result is difficult to reconcile with *JDS Uniphase Corp. v. Jennings*,[3] which applied California law to a breach of a confidentiality agreement between a California corporation and a Virginia employee. The employee argued—much like the defendant in *Erhart*—that California prohibited enforcement of the confidentiality agreement as a matter of public policy because it would impede his pursuit of SOX and other whistleblower claims. The district court held that the California public policy declaration did not address the enforceability of confidentiality agreements and did not, in any event, "authorize disgruntled employees to pilfer a wheelbarrow full of an employer's proprietary documents in violation of their contract merely because it might help them blow the whistle on an employer's violations of law…"[4] The court recognized that

3 473 F. Supp. 2d 697 (E.D. Va. 2007).

4 473 F. Supp. 2d at 702.

circumstances can arise that call for extraordinary measures to prevent destruction of evidence valuable to the whistleblower or law enforcement, but noted that the plaintiff had not raised such an issue. The court ordered the return of the employer's documents pending the ordinary course of civil discovery.

Both *Erhart* and *Jennings* involved individual employees asserting personal claims of unlawful retaliation against their employer, although their whistleblower claims had at least a semblance of a public interest claim. When the plaintiff-employee asserts a claim of fraud on behalf of the federal government as a relator under the False Claims Act (FCA),[5] the public interest is more obvious. In a *qui tam* case under the FCA, the plaintiff—referred to as a "relator" in FCA parlance—sues in the name of the United States government. The statute contains a series of procedural requirements involving notice to the Department of Justice (DOJ), and the DOJ has an opportunity to intervene in and take over the lawsuit. The relator in a successful FCA case has a right to 15-30 percent of any government recovery. Courts have shown greater solicitude for the DOJ's access to evidence of fraud in FCA cases than for an individual's right to hold onto the employer's information in other types of cases. Likewise, courts are less impressed with confidentiality agreements when the government's right to recover from a fraudster is at issue.

In *United States ex rel. Grandeau v. Cancer Treatment Centers of America*,[6] the plaintiff-relator brought a *qui tam* action alleging the defendant, a medical company, had engaged in fraudulent billing practices in violation of the FCA. After the court unsealed the *qui tam* complaint, the employer learned that the plaintiff had collected, copied, and delivered numerous documents to the government. The defendant filed a counterclaim for, among other things, breach of the relator's confidentiality agreement. The court dismissed the counterclaim, holding that the FCA's policy of protecting whistleblowers shielded the plaintiff from liability related to his removal of improperly obtained documents that supported his *qui tam* action.

The court reached a similar result in *United States ex rel. Ruhe v. Masimo Corp.*,[7] in which the plaintiffs-relators were former sales representatives for the defendant. While quitting their employment, plaintiffs copied and moved—in violation of their non-disclosure agreements—evidence from their hard drives for the purpose of providing these documents to the government to corroborate their claims of alleged fraud by the defendant. As part of the defendant's motion to dismiss, it sought to strike the information derived from the purloined documents as scandalous and impertinent: scandalous because the documents were taken and disclosed in violation of plaintiffs' confidentiality agreements, and impertinent because the allegations were unnecessary to the FCA claims.[8] The district court rejected the employer's position, holding that neither the documents nor the circumstances of their removal were scandalous or impertinent because the plaintiffs "sought to expose a fraud against the government and limited their taking to documents relevant to the alleged fraud. Thus, this taking and publication was not wrongful, even in light of non-disclosure agreements."[9] The court also noted that the relators took only the documents they would need to maintain their FCA case.

5 31 U.S.C. §§ 3729-33.
6 350 F. Supp. 2d 765 (N.D. Ill. 2004).
7 929 F. Supp. 2d 1033 (C.D. Cal. 2012).
8 *Id.* at 1038.
9 *Id.* at 1039.

A non-disclosure agreement was similarly unavailing in the early stages of *X Corp. v. Doe*,[10] a multi-part controversy involving a member of a company's in-house legal staff who had taken documents while still employed so he could bring a *qui tam* action after he lost his job. The attorney—like many employees—had executed an "Employment, Invention and Confidential Information Agreement," which required him " (i) to return to [the employer] all records obtained during, or in connection with, his employment and (ii) to preserve [the employer]'s confidential information."[11] Throughout his employment, the attorney received privileged and confidential information in order to provide legal advice. The employer terminated the lawyer, who alleged the termination was in retaliation for actions the company perceived as actions in furtherance of a possible *qui tam* lawsuit.[12] Upon his termination, the lawyer made copies of documents that he alleged revealed the company was defrauding the federal government. The employee's lawyer sent a demand letter to the company, attaching a draft complaint, which contained specific references to and excerpts from the company's "confidential" documents. The company responded with a preemptive suit for: (1) breach of fiduciary duty by allegedly revealing confidences to the lawyer's own attorney; (2) breach of the confidentiality agreement; (3) recovery of the allegedly misappropriated documents and records; (4) injunctive relief to prevent disclosure of alleged confidential information in his personal claim against the company or for any purpose; and (5) a declaratory judgment that the employee may not disclose the confidential information.[13] In deciding the company's motion for a preliminary injunction and to enjoin the defendant to return the documents, the court held that public policy did not favor the return of documents to the moving party at the early stage of litigation because there had been insufficient time to determine whether the documents established fraud. The court noted that any contrary ruling would allow a party to "rely on [a non-disclosure agreement] to conceal illegal activity."[14]

In *Shmushkovich v. Home Bound Healthcare, Inc.*,[15] plaintiffs-relators brought a *qui tam* case against their employer alleging that the employer had knowingly submitted false claims for payment to Medicare in violation of the FCA. Upon placing plaintiff on leave after the unsealing of the FCA *qui tam* complaint, the employer requested that the relators return all of its property, including electronic files the relators possessed in order to perform their job duties. In response, the relators purchased hard drives and created encrypted copies of the requested files. One of the relators returned a hard drive with the requested documents to the employer but gave a second hard drive to his attorney, who kept it in a sealed envelope. The relator was then terminated. The employer filed a motion requesting that the court order the relator to return the employer's property (originals and copies). The company argued that the plaintiff engaged in self-help discovery by retaining documents outside the bounds of formal discovery.

The court noted that, although Congress contemplated the need for relators to obtain and produce confidential corporate documents, the protection afforded to self-help discovery in FCA cases is limited to material reasonably related to the formation of a case.[16] The court allowed the relators to retain documents reasonably related to their FCA claims, but ordered them to destroy documents in their possession that were not relevant to his FCA claims. The court directed the relators to prepare a schedule of documents and other information they had taken and allowed the defendant-employer to challenge the relevance of the documents to the FCA claims. Recognizing

10 805 F. Supp. 1298 (E.D. Va. 1992).

11 *Id.* at 1300.

12 See 31 U.S.C. § 3730(h), the anti-retaliation provisions of the FCA.

13 *Id.* at 1301-02.

14 *Id.* at 1310 n.24. The district judge in the *John Doe* cases is the same judge who later decided the *Jennings* case discussed above.

15 No. 12 C 2924, 2015 U.S. Dist. LEXIS 81389 (N.D. Ill. June 23, 2015).

16 *Id.* at *6.

the employer's interest in the information, the court also ordered that the information be held confidentially and not used for any purpose except the FCA action.

In *United States ex rel. Rector v. Bon Secours Richmond Health Corp.*,[17] the defendant obtained the return of its information, but the court required preservation of the information for later use through examination by an independent expert.

The relator was a former employee of an employment agency that contracted with the defendants. He filed a *qui tam* complaint under seal. The relator's counsel then met with another former employee of the defendant, who provided plaintiff's counsel with the defendant's electronic documents, two desktop computers, and a laptop hard-drive backup. The defendant contended that the computers and documents contained defendant's trade secrets as well as confidential patient logs. The company filed a motion to: (1) return all of its data; (2) permit a computer forensic consultant to image any and all computers or data devices in the plaintiff's possession, custody, or control that contained the data at issue; (3) verifiably delete such data from all such computers or data devices; and (4) individually prepare affidavits identifying every item of defendant's data in their possession, custody, or control. The court directed plaintiff to return and delete all company data. The court stated, "[i]t is true that the FCA contemplates whistleblower possession of documents obtained from employers that evidence fraud upon the government … However, the FCA does not permit whistleblowers to have carte blanche to acquire such information in any way they deem necessary."[18]

An interesting twist on this theme in the Title VII arena is *Ashman v. Solectron Corp*.[19] Shortly after plaintiff's termination from his former employer, he filed an age and disability discrimination complaint with the Equal Employment Opportunity Commission (EEOC). As part of the complaint process, the plaintiff provided the EEOC with documents that he had obtained while employed. The plaintiff also provided the EEOC with documents he obtained using his old computer network login. The plaintiff was subsequently arrested and admitted that he had been accessing the defendant's internal emails and other documents in order to obtain evidence to bolster his EEOC complaint. The district court in the discrimination case ordered the plaintiff to return all improperly obtained documents, although ultimately it allowed him to obtain many of the same documents through the normal course of civil discovery.

B. A counterclaim against an employee for breach of the employee's confidentiality agreement may be maintained against a relator if the employer has suffered damage apart from the FCA suit itself.

While employers have been largely unsuccessful in securing the return of their confidential but possibly incriminating documents in the face of a whistleblower claim, they have had some modest success in maintaining counterclaims for damages that might result from an employee's breach of the confidentiality agreement if the damage is independent of the *qui tam* action.[20]

As an initial matter, an employer cannot counterclaim against the relator for indemnification or contribution for FCA damages ordered against the employer.[21]

However, it is sometimes possible to maintain a counterclaim for damages independent of the FCA damages, and the likelihood of success for the employer is greater if the employee has taken documents not related to the subject of the FCA case. An important counterclaim decision is

17 No. 3:11-CV-38, 2014 U.S. Dist. LEXIS 1031 (E.D. Va. Jan. 6, 2014).

18 *Id.* at *18.

19 2008 U.S. Dist. LEXIS 98934 (N.D. Cal. Dec. 1, 2008

20 *United States ex rel. Mossey v. Pal-Tech, Inc.*, 231 F. Supp. 2d 94, 99 (D.D.C. 2002); *see also United States ex rel. Battiata v. Puchalski*, 906 F. Supp. 2d 451, 460-61 (D.S.C. 2012).

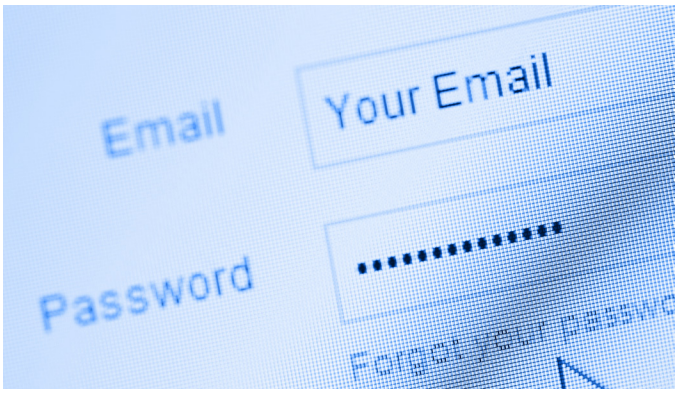
21 *See, e.g., Walsh v. Amerisource Bergen Corp.*, No. 11-7584, 2014 U.S. Dist. LEXIS 82064 (E.D. Pa. June 16, 2014); *United States v. Campbell*, No. 08-1951, 2011 U.S. Dist. LEXIS 1207, at **29-30 (D.N.J. Jan. 4, 2011); *United States ex rel. Miller v. Hill Harbert Int'l Constr., Inc.*, 505 F. Supp. 20, 26 (D.D.C. 2007).

United States ex rel. Cafasso v. General Dynamics C4 Systems, Inc.,[22] in which the court granted judgment against a failed *qui tam* relator on the company's counterclaim for theft in violation of a confidentiality agreement. *Cafasso* turns in part on the amount of information removed by the employee that was unrelated to her *qui tam* action, and in part on the dismissal of the underlying *qui tam* action itself for failure to state a claim. The court observed that public policy might justify an exception to enforcement of confidentiality agreements in FCA cases, but that the plaintiff's "vast and indiscriminate appropriation" of the company's confidential material made application of an exception inappropriate in that case.[23] It was this discussion in *Cafasso* of the possible exception in the FCA context that enabled the district court in *Erhart* to distinguish *Cafasso* and advance the cause of whistleblowing in California.

Other cases in which counterclaims for breach of a confidentiality agreement have survived at the Rule 12(b)(6) stage include *United States ex rel. Wildhirt v. AARS Forever, Inc.*[24] and *United States ex rel. Brianna Michaels and Amy Whitesides v. Agape Senior Community Inc.*[25]

C. Does breach of the attorney-client privilege or an attorney's duty to maintain confidences provide a better argument for requiring a former employee to return information?

The saga of "John Doe" and "X Corporation," a trio of district court decisions between August 1992 and September 1994, illustrates the problems that can arise for both sides when an employee removes the employer's confidential information, but with the added complication that John Doe was an attorney for the corporation who sought to bring a *qui tam* action against his former employer-client using information he had obtained through the attorney-client relationship.



In *X Corp. v. John Doe*,[26] the corporation had terminated Doe's employment. Doe retained counsel, who sent X Corp. a demand letter with a draft Virginia wrongful discharge complaint that included excerpts from X Corp.'s confidential documents, which Doe had removed and provided to his attorney. X Corp. responded with a lawsuit that asked for Doe to be enjoined from further disclosure of its information and to return that information to the company.

Although the court rejected the company's attempt to get its documents back at the outset of the litigation, the court accepted the proposition that Doe was using confidential documents for litigation purposes and enjoined further disclosure except to his attorney and except for purposes of the litigation.[27] The court held that under the crime-fraud exception to the privilege, Doe would ultimately be obligated to return the documents unless a reasonable attorney would believe that the disputed information "clearly established" his employer-client's fraud against the government.

Doe then filed both a state court wrongful discharge action and a retaliation counterclaim under the anti-retaliation provision of the FCA. He also filed a *qui tam* action under the FCA that depended largely on the confidential information he possessed as part of his role as in-house attorney and took with him when X Corp. laid him off.

22 637 F.3d 1047 (9th Cir. 2011).
23 637 F.3d at 1062.
24 No 09-1215, 2013 U.S. Dist. LEXIS 133982 (N.D. Ill. Sept. 19, 2013).
25 No. 12-3466, 2013 U.S. Dist. LEXIS 171518 (D.S.C. Dec. 5, 2013).
26 805 F. Supp. 1298 (E.D. Va. 1992); *see also supra* note 10 and accompanying discussion.
27 805 F. Supp. at 1302 n.5.

After several months of discovery and cross-motions for summary judgement, the court returned to the question of the crime-fraud exception.[28] The district court analyzed but eventually rejected the lawyer's argument that he had established that his employer had defrauded the government. The court concluded that it was not reasonable for an attorney in his position to have believed that he had uncovered a fraud. Because he did not meet this threshold issue, he could not meet the crime-fraud exception.

Because Doe failed to establish the crime-fraud exception, the district court ordered him to return the privileged documents to his former employer-client and enjoined the government to return to X Corp. the privileged documents Doe had provided. In the same decision, the court granted summary judgment in favor of the employer on the FCA retaliation claims. Surprisingly, under the circumstances, the court held that Doe had not established that he had initiated or in any way assisted in the filing of a *qui tam* action, which in 1992 was the FCA definition of protected activity.[29] Doe had secretly copied and removed numerous confidential documents while he was an employee but, as the court observed, this was done in secret and no one from the company was aware of Doe's activities until after he was gone. Lacking a causal connection to establish liability for retaliation, the court entered judgment in the employer's favor.

The final indignity for John Doe was delivered in the FCA case. During the period after Doe had served his complaint on the government but before the deadline for the government to intervene, the company and the government settled the FCA action. X Corp. then objected to Doe's participation as a relator in the settlement proceeds because, it contended, his previous role as company counsel and his use of privileged documents precluded him from serving as a relator. In *United States ex rel. John Doe v. X Corp.*,[30] the court first held that the FCA contained no prohibition on a lawyer serving as a relator. Nonetheless, the court held that it was a violation of the Rules of Professional Conduct for the lawyer to use information he had obtained through his confidential relationship with the client to the client's detriment. The court then precluded Doe from being a relator because it was "only through confidential communications with X Corp. employees and by review of some confidential documents that Doe learned all of the alleged facts supporting his allegations" of fraud.[31]

After two years of litigation, the government got what it needed to negotiate a settlement of whatever FCA liability it saw on the part of the employer. The company preserved its trade secrets and confidential information, except for what appeared in the record of the case. The attorney-turned-relator ended up with nothing.[32]

Quite a different outcome occurred in *Wadler v. Bio-Rad Laboratories, Inc.*,[33] a SOX, Dodd-Frank, and California law case brought by a former general counsel who had, while employed, repeatedly made internal complaints about Foreign Corrupt Practices Act violations in China.

Prior to a 2017 trial, the parties had participated in two "independent" law firm investigations, a DOL SOX investigation, and proceedings before the SEC. The great majority of the documents

28 *X Corp. v. John Doe*, 816 F. Supp. 1298 (E.D. Va. 1993).

29 The phrase "stop 1 or more violations" of the FCA did not appear in the statute until 2009. Had the current language been in effect in 1992, it is less likely that the court would have dismissed the complaint as easily as it did in this decision.

30 862 F. Supp. 1502 (E.D. Va. 1994).

31 *Id.* at 1509-10.

32 The reported decisions do not state the basis for the government's decision to settle. As noted above, the district court was not impressed with the merits of the FCA claim as pleaded by Doe.

33 212 F. Supp. 3d 829 (N.D. Cal. 2016).

and most of the testimony to be offered at trial consisted of privileged written and oral communications between the company and its attorneys, including the plaintiff. In an effort to avoid the spectacle of a public airing of the company's attorney-client communications and confidential information, the company's attorneys moved to preclude the plaintiff from using "protected information" at the trial, including testimony the plaintiff "learned in the course of his services as [the company's] general counsel." Had the court granted the motion, it would have effectively prevented the plaintiff from presenting his case. The court denied the motion with an extensive analysis of the myriad attorney-client privilege issues surrounding the case.

First, the court held that the California law of attorney-client privilege, explained definitively in *General Dynamics Corp. v. The Superior Court of San Bernardino County*,[34] which bars an in-house attorney from maintaining a common law wrongful discharge action against the company-employer, does not apply to a federal SOX retaliation claim. The court then reviewed federal common law on the use of privileged information in whistleblower proceedings and concluded that it was permitted if the plaintiff reasonably believed that the information was necessary to prove a claim or defense. The court relied heavily on *VanAsdale v. International Game Technology*[35] and *Kachmar v. SunGard Data Systems, Inc*.[36] Thus, rather than protecting the confidential information of the employer-client, the court allowed the use of such information in the SOX/Dodd Frank proceeding provided it was reasonable for the plaintiff-attorney to use it to win his case. The court went on to find that the defendant had waived the privilege as to numerous pieces of evidence used in prior proceedings before the SEC and the DOL, and in the federal court litigation itself.

Ultimately, a jury awarded the plaintiff $2.96 million in back wages and $5 million in punitive damages.[37]

D. The future is here: The Defend Trade Secrets Act's whistleblower immunity provisions likely will impact many of these disputes, which may not be good news for employers confronted with a whistleblower intent on removing information from company files to use in a lawsuit or to report to a government official.

On May 11, 2016, Congress amended the Economic Espionage Act by enacting the DTSA to provide a federal civil remedy for employers to use against current and former employees, contractors, and others who unlawfully misappropriate the employer's trade secret information. Since the DTSA's enactment, numerous federal courts have granted injunctive relief to former employers against trade secret misappropriators.

For instance, there are now numerous cases across the country where employers have been successful in obtaining injunctions for violations of the DTSA. Notably, one key to these successful DTSA cases has been a strong pre-suit forensic foundation of the information that was taken. This backdrop has allowed the employer to show the court exactly what information was taken, why it was secret, and how it will harm the company by being used or disclosed outside the company. Merely alleging a taking or expressing a fear of harm due to a disclosure is not enough.[38]

With a solid pre-suit factual foundation, numerous employers have been successful in obtaining injunctions under the DTSA. In *Engility Corp. v. Daniels*,[39] the plaintiff former employer alleged that a separated employee stole information before joining his new company and was prepared to use that information to poach a large client. The court granted the former employer's request

34 7 Cal. 4th 1164 (Cal. 1994).

35 577 F.3d 989 (9th Cir. 2009).

36 109 F.3d 173 (3d Cir. 1997).

37 *Wadler v. Bio-Rad Labs., Inc.*, No. 15-cv-2356 (Feb. 2, 2017) (Jury Verdict, Docket No. 223).

38 *See, e.g.*, *Phyllis Schlafly Revocable Trust v. Cori*, No. 4:16-cv-1631, 2016 U.S. Dist. LEXIS 155409, at *11 (E.D. Mo. Nov. 9, 2016) (finding the plaintiff's fear that employees may have copied all or part of a database too speculative to show immediate and irreparable harm).

39 No. 16-cv-2473, 2016 U.S. Dist. LEXIS 166737, at **30-31 (D. Colo. Dec. 2, 2016).

for an injunction under the DTSA. The injunction prohibited the former employee and his new employer from disclosing any of the confidential information, imposed a nationwide non-compete for one year, and provided that defendants could not solicit business from one of the plaintiff employer's biggest contracts.

Similarly, in *T&S Brass and Bronze Works, Inc. v. Slanina*,[40] the former employer obtained an injunction in an egregious case of trade secret theft. The defendants-former employees had "disclosed product designs, sales, and other financial data, and customer information" to both competitors and companies with an interest in purchasing the plaintiff's company. One defendant had provided proprietary hardware to foreign companies and routinely lied about his whereabouts. The court's injunction prevented the deletion, destruction, use, or modification of any trade secrets, enjoined the defendants from violating the various agreements they had violated, precluded them from competing or using their new name (including the foreign company they started), barred them from disparaging the plaintiff, and forbade them from entering into employment relationships with similar companies.

Also, in *Mickey's Linen v. Fischer*,[41] the plaintiffs obtained an injunction where a former employee violated numerous company policies as he was leaving the company, including wiping his phone, allegedly shredding stacks of documents he was required to return, and lying about the identity of his next employer. The injunction required, among other things, the defendant to return to the plaintiff all of its customer and business-related information, including all documents and other materials prepared at, by, or for the plaintiff, and all copies and duplicates of the same. He also was ordered to return all electronic copies, if any existed, he had deleted. He further was ordered not to use or disclose his former employer's confidential customer or business information.

Note that none of the foregoing DTSA cases involved a whistleblower or the assertion of the DTSA's "immunity" provisions as a defense to the misappropriation of the former employer's internal trade secret information. But, uniquely, the DTSA does expressly provide legal immunity for employees and former employees who take their employer's trade secret information *for a specific purpose* and who only disclose the information *in a specific way*. Here's how the DTSA's immunity provisions work.

In the DTSA's immunity provisions, Congress recognized the equally important but conflicting policies between encouraging whistleblowing and protecting trade secrets. Toward encouraging whistleblowing, the DTSA includes both civil and criminal immunity protection for whistleblowers. The immunity protects whistleblowers who misappropriate and disclose trade secret information, but only for specific reasons and in specific ways as defined in the DTSA. Specifically, 18 U.S.C. § 1833(b) provides:

> An individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that:
>
> a. Is made: (i) in confidence to a Federal, State or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law OR;
>
> b. Is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal.

Thus, absent compliance with § 1833(b)'s narrow protections, a current or former employee's misuse or disclosure of an employer's internal "trade secret" information—without the employer's prior consent and authorization—violates the EEA and parallel state *trade secret laws*. The DTSA's civil and criminal immunity protections do not apply to unauthorized misappropriations outside of § 1833(b); in that event, the trade secret misappropriator is exposed to the EEA's criminal

40 No. 6:16-3687, 2016 U.S. Dist. LEXIS 186427, at *22 (D.S.C. Dec. 20, 2016).

41 No. 17 C 2154, 2017 U.S. Dist. LEXIS 145513 (N.D. Ill. Sept. 8, 2017).

penalties, which can be severe, and to the DTSA's and state-law civil remedies. Moreover, keep in mind that the DTSA grants immunity from liability only for violations of federal or state *trade secret law*. It does not grant legal immunity for breaching a non-disclosure agreement, violating computer use laws, or abridging other applicable laws.

Consequently, for the run-of-the-mill "grab and bolt" misappropriation of trade secrets by a former employee who joins a competitor—and who has taken the information without authorization and solely for competitive business purposes—there appears to be no legal immunity or other protection under the DTSA or under any other relevant laws.

To date, research has uncovered only one federal court case that has addressed the DTSA's immunity provisions in the context of litigation involving a whistleblower. In *UNUM Group v. Loftus*,[42] the court denied the former employee's motion to dismiss a DTSA claim brought by the former employer. Noting that the DTSA's immunity provision acts as an affirmative defense, the court held that the record at the dismissal stage must contain facts that can support or undermine the immunity defense. According to the court, these facts include, but are not necessarily limited to: (1) the significance of the documents taken; (2) whether a lawsuit has been filed by the employee using that information; (3) whether or not the employee turned over any and all documents to his or her attorney or the government; (4) which documents were taken; and (5) the plans for the use of those documents. According to the court, it is up to the whistleblower to provide this information. Because the whistleblower had failed to do so, the employer obtained an injunction, which obligated the whistleblower to turn over all documents taken from the employer and to destroy all copies of those documents.[43]

Note that the *UNUM* case may have had a different result had the whistleblower been the first to file and therefore could have presented his set of facts in a complaint. Moreover, other employers should not blindly rely on *Unum*. Generally, when Congress immunizes an actor based on the actor's conduct, courts enforce that immunity at the earliest possible stage in the litigation. This approach furthers the policy reasons underlying the grant of immunity, which exists to allow the whistleblower to be free from suit, including the time commitment and legal defense costs thereof. In *Unum*, the court essentially forced the whistleblower to waive immunity protection in favor of asserting immunity as an affirmative defense.

Finally, there are, as yet, no reported DTSA immunity decisions arising in the context of a *qui tam* action.

42 220 F. Supp. 3d 143 (D. Mass. 2016).

43 *But see Christian v. Lannett Co., Inc.*, No. CV 16-963, (E.D. Pa. Mar. 29, 2018) (in a Title VII, ADA, and FMLA disparate treatment and failure-to-accommodate employment termination case, the court dismissed the employer's DTSA counterclaim against the plaintiff who provided 22,000 pages of the employer's internal documents to her legal counsel, who subsequently produced the documents in discovery; the court found this disclosure was made "in confidence … to an attorney … solely for the purpose of reporting or investigating a suspected violation of law" pursuant to the DTSA's immunity provision in 18 U.S.C. §1833(b)).

II. POTENTIAL CONSEQUENCES FOR AN EMPLOYEE WHO COLLECTS AND REMOVES CONFIDENTIAL INFORMATION

Employers often want to take action against employees who depart with company secrets or privileged information. The scenarios presented in this area are very fact-intensive, and employers should proceed with great care in formulating plans to "sanction" a departing employee.

A. Prosecution: possible but rare

Employers frequently ask whether an employee who breaks into company file cabinets or accesses company computer systems is liable to prosecution by a local district attorney or the U.S. Attorney's office. The answer to this question is sometimes "yes," but the employer that chooses this route must be aware of three risks that may not be obvious at the outset. First, the criminal investigative process may not be swift; it certainly will not be as swift as a civil suit and a motion for preliminary injunction. Second, by seeking a prosecutor's help, the employer is surrendering control over the process. Prosecutors tend to move when they want to move and not necessarily in the direction the employer wants. Third, if the information taken by the employee tends to show criminal activities by others still at the company, the report to law enforcement may have an unintended boomerang effect. Nevertheless, a criminal conviction may be worth it if it succeeds. The following are some examples.

In *State v. Saavedra*,[44] an employee of the North Bergen Board of Education (Board) filed an action asserting statutory and common law employment discrimination claims against the Board. In discovery, defendant's counsel produced several hundred documents that allegedly had been removed or copied from Board files. According to the Board, the documents included highly confidential student educational and medical records that were protected by federal and state privacy laws. The Board reported the alleged theft to the county prosecutor.

The prosecutor presented the matter to a grand jury, where a Board attorney testified about the defendant's position with the Board, the Board's discovery through the civil litigation that the defendant possessed documents from its files, and the privacy implications of the alleged appropriation. The grand jury indicted the defendant for official misconduct and theft by unlawful taking of public documents.

Before the state supreme court, the defendant-employee argued that the theft of documents was protected activity under the New Jersey anti-discrimination statutes, invoking *Quinlan v. Curtiss-Wright Corp*.[45] The Supreme Court of New Jersey acknowledged its own *Quinlan* decision, but refused to give the employee the right to commit what would otherwise be a crime in the name of pursuing a discrimination lawsuit.

Two other cases are significant, but do not arise in the context of whistleblower actions. In *United States v. Nosal*,[46] the defendant-employee began creating a competing business while still employed. He downloaded confidential and trade secret information from his former employer that he intended to use for his new business. Upon leaving the company, having had his network login revoked, the defendant used his former assistant's login credentials and continued accessing documents. Once the former employer became aware, it turned the matter over to the U.S. Attorney's Office. The defendant was indicted, and convicted, under the Computer Fraud and Abuse Act (CFAA) and the EEA. The U.S. Court of Appeals for the Ninth Circuit held that the defendant violated the CFAA because he was without authorization to access the information, as the company had rescinded his permission to access the computer upon his separation.

In *United States v. Aleynikov*,[47] the defendant was charged with stealing and transferring his

44 117 A.3d 1169 (N.J. 2015).
45 8 A.3d 209 (N.J. 2010).
46 828 F.3d 865 (9th Cir. 2016).
47 676 F.3d 71 (2d Cir. 2012).

employer's proprietary computer source code in violation of the National Stolen Property Act (NSPA) and the EEA. After a jury convicted the defendant on both counts, he appealed to the U.S. Court of Appeals for the Second Circuit. The defendant argued that source code did not fit in the definition of "good" within the meaning of the NSPA, nor was the source code "related" to a product "produced for or placed in interstate or foreign commerce" within the meaning of the EEA. The Second Circuit agreed and reversed the judgment on both counts. In so holding, the court determined that purely intellectual property was not considered a "good," whereas the language of the NSPA and previously prosecuted cases contemplate only tangible goods. In reversing the conviction under the EEA, the court held that the source code was not a trade secret that was "related to or included in a product that is produced for or placed in interstate or foreign commerce."[48]

The EEA has been amended to correct the *Aleynikov* decision.[49] The defendant, Aleynikov, was also prosecuted by the State of New York and convicted. In May 2018, the state's highest court affirmed his conviction for the unlawful use of secret scientific material—holding that by copying the source code to a physical hard drive, the defendant had made a "tangible" reproduction even though source code, itself, is intangible "[b]y its very nature."[50]

B. Litigation sanctions

Dismissal of a whistleblower action is not a favored remedy, and under the FCA, the government's involvement means that the dismissal of the relator may not end the litigation. However, the *X Corp. v. John Doe* litigation[51] is one example where an FCA relator lost his claims altogether because of the ethical problems presented by his removal of and reliance upon confidential documents.

The U.S. Court of Appeals for the Second Circuit decision in *United States ex rel. Fair Laboratory Practices Associates v. Quest Diagnostics*,[52] shows that the courts continue to scrutinize the behavior of lawyers and will not ordinarily allow them to use client confidential information to profit through the *qui tam* provisions of the FCA.

The relator in this action was a partnership formed by three former executives of an acquired entity; the partnership arose for the express purpose of suing their former employer and, moreover, the company that bought it. The former general counsel was one of the partners, and was apparently the principal source of the information that enabled the relator to move forward. The defendant company recognized that their former lawyer was using its confidential information to its detriment and moved to dismiss the case. As the judge had done 20 years earlier, the district court out of New York first addressed—and rejected—the relator's contention that the public interest in fostering FCA disclosures preempts state ethical rules.

On appeal, the Second Circuit concluded that the former general counsel had violated Rule 1.9(c) of the New York Rules of Professional Conduct by disclosing client confidences in order to pursue the *qui tam* action. In rejecting the attorney's claim that he had revealed only as much information as necessary to prevent the defendant from committing a crime, the court found that he had in fact revealed significantly more information than was necessary to forestall any crime he suspected. Finally, the Second Circuit affirmed the district court's exercise of its discretion in disqualifying:

48 *Id.* at 79.

49 *See United States v. Agrawal*, 726 F.3d 235, 244 n. 7 (2d Cir. 2013); *see also* Theft of Trade Secrets Clarification Act of 2012, Pub. L. No. 112-236, 126 Stat. 1627 (providing for EEA to be amended to strike phrase "or included in a product that is produced for or placed in" and to insert phrase "a product or service used in or intended for use in," so that relevant language now reads: "Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce . . . ."); 158 Cong. Rec. S6978-03 (daily ed. Nov. 27, 2012) (statement of Sen. Leahy) (observing that *Aleynikov* decision "cast doubt on the reach" of EEA, and that "clarifying legislation that the Senate will pass today corrects the court's narrow reading to ensure that our federal criminal laws adequately address the theft of trade secrets" (emphasis added)).

50 *People v. Aleynikov*, 2018 N.Y. LEXIS 1079, at *1 (N.Y. May 3, 2018).

51 *See supra* Part I.C.

52 734 F.3d 154 (2d Cir. 2013).

(a) the attorney and the *qui tam* partnership from acting as relators and thereby representing the U.S. government; and (b) the relators' counsel because of the information the former general counsel had conveyed to them. The court also upheld the district court's dismissal of the *qui tam* action in its entirety due to the ethical breach. As the appellate court noted, the dismissal of the *qui tam* action did not foreclose a government action, and eventually the defendant settled FCA claims threatened by the government.[53]

In *Glynn v. EDO Corp.*,[54] meanwhile, the court awarded sanctions of $20,000 against the plaintiff and plaintiff's attorney as a result of the plaintiff's misconduct in obtaining his employer's confidential information and documents. After plaintiff's termination, he continued communication with a fellow co-worker, who sent plaintiff internal documents and emails. Plaintiff subsequently forwarded some of these documents to his attorney. He then filed suit under the FCA for retaliation based on his communications, while still employed with defendants, with a government investigator relating to defendants' business practices. Defendants filed counterclaims and crossclaims for breach of contract, misappropriation of trade secrets, breach of fiduciary duty, conversation defamation, tortious interference, violation of New Hampshire's consumer protection statute, unjust enrichment, and civil conspiracy. The court found that defendants proved by clear and convincing evidence that on at least a few occasions, plaintiff and his counsel wrongfully acquired non-public, internal information.

The defendant seeking sanctions did not prove that it was or would be sufficiently prejudiced enough to warrant dismissal. (Such a remedy is disfavored in any event, as courts recognize that there is an important public policy in resolving claims on their merits.) Moreover, according to the court, any information helpful to plaintiff's case that had been improperly acquired likely would have been acquired through discovery anyway, and therefore continued prejudice was minimal. Additionally, plaintiff obtained only a "handful" of documents improperly. The court imposed sanctions of $20,000, both to punish the plaintiff and counsel for their misconduct and to mitigate the defendant's costs in bringing a motion for sanctions.[55]

In *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, L.L.C.*,[56] the plaintiffs sought damages and injunctive relief, "accusing [d]efendants of (1) stealing [p]laintiffs' business model, customers, and internal documents, (2) breaching employee

53 This result might seem at odds with the *Wadler* decision (*see supra* Part I.C.), since the *Wadler* court allowed the claims to proceed even though the plaintiff's case consisted almost entirely of privileged information. The only differences appear to be that: (1) one case was decided under California law, the other under New York law; and (2) Wadler was not acting as a representative of the government.

54 No. JFM-07-01660, 2010 U.S. Dist. LEXIS 86013 (D. Md. Aug. 20, 2010).

55 The district court eventually granted summary judgment against Glynn, which the U.S. Court of Appeals for the Fourth Circuit upheld in *Glynn v. EDO Corp.*, 710 F.3d 209 (4th Cir. 2013).

56 587 F. Supp. 2d 548, 565 (S.D.N.Y. 2008).

fiduciary duties, and (3) infringing [p]laintiffs' trademarks, trade-dress, and copyrights."[57] The defendants-former employees counterclaimed, alleging violations of the New York labor law, the Stored Communications Act, and the Electronic Communications Privacy Act. They also complained of attempted sabotage of defendants' business and unauthorized use of defendants' images in violation of New York privacy law.

In addition, defendants sought sanctions arising out of plaintiffs' unauthorized access to 34 of the former employees' emails. The former employees' username and password information remained saved on the company computer. Plaintiffs relied heavily on the emails, considering them crucial to its case. Some of the emails improperly obtained by plaintiffs were contemporaneous with the underlying lawsuit and were between the former employee and the defendant's law firm.

The court noted in this case that the sanctions available under the Federal Rules of Civil Procedure were not directly applicable, as the misconduct (the improper acquisition of documents) occurred prior to the lawsuit and outside the normal discovery process. Nonetheless, the court stated:

> Federal courts do have inherent equitable powers of courts of law over their own process, to prevent abuses, oppression, and injustices . . . Courts may impose sanctions and rely upon their inherent authority even where the conduct at issue is not covered by one of the other sanctioning provisions. Furthermore, a district court may resort to its inherent power to fashion sanctions, even in situations similar or identical to those contemplated by [a] statute or rule.[58]

The emails, which were improperly obtained by the plaintiffs' owner after logging into the former employee's account, were ordered to be precluded from trial, except for impeachment purposes.

C. Termination of employment for violation of employer policy or confidentiality agreement

Ten years ago (but perhaps not today) an employment attorney could safely predict that an employee who stole an employer's documents could be terminated without fear of retaliation liability—even if the employee's intent was to use those documents to pursue a discrimination claim. Notably, the principal federal whistleblower statutes limit their protection to "lawful" acts by employees in furtherance of their claims.[59]

In *Niswander v. Cincinnati Ins. Co.*,[60] the plaintiff was involved in a class action lawsuit under the Equal Pay Act and Title VII against the defendant. The class-action lawyers had requested that all the class members submit any documents that related to their employment, and any documents that related to the allegations made in their pleadings. In response, the plaintiff gathered up documents from her home (where she worked) and sent them to the attorneys. She believed the documents she submitted were relevant to the defendant's alleged retaliation against her for participating in the lawsuit. Retaliation was not a claim brought in the class action, although it was being discussed as a possible new claim. Moreover, the documents did not themselves show retaliation, but were meant to "jog her memory" as to the retaliation she believed she endured as a result of her participation in the lawsuit. The documents submitted included confidential information, including sensitive client information. Importantly, in her deposition, plaintiff admitted that at the time she did not have documents to support an equal pay claim. The employer fired her for stealing the documents.

57 *Id.* at 551.

58 *Id.* at 568 (internal quotations and citations omitted).

59 *See, e.g.*, 18 U.S.C. § 1514(a) (SOX); 15 U.S.C. § 78u-6(h)(1)(A) (Dodd-Frank); 31 U.S.C. 3730(h) (FCA).

60 529 F.3d 714 (6th Cir. 2008).

On appeal, the court identified the following factors for determining whether plaintiff's delivery of confidential information was reasonable:

> (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.[61]

Consistent with these principles, the appellate court reviewed the district court's ruling in favor of the employer. In determining whether plaintiff was opposing unlawful conduct under the EPA and Title VII, and therefore engaging in protected activity, the lower court held:

> that Defendant's interest in ensuring compliance with its policies of privacy and the law, and maintaining the confidentiality of its clients' personal information outweighs Plaintiff's interest in preserving what she considered to be evidence of unlawful retaliation on the part of Defendant. This is so especially in light of the fact that Plaintiff could have preserved this evidence without violating the law and her employer's policy and trust as she could have taken notes of the incidents that she felt spurned retaliation instead of taking pictures and claims file information that jogged her memory of these incidents and giving them to her attorney. Moreover, this "evidence" that Plaintiff handed over to her attorney does not prove retaliation in and of itself as Plaintiff herself admitted that the documents that she gave her attorney relating to claims file information only served to trigger her memory about incidents which she believed constituted retaliation.[62]

The court ultimately affirmed the district court's grant of summary judgment on plaintiff's retaliation claim. Moreover, the court held that defendant was lawfully permitted to terminate her for dissemination of its confidential information.

O'Day v. McDonnell Douglas Helicopter Co.,[63] is an age discrimination case involving stolen documents. After being denied a promotion, the plaintiff "rummaged" through and copied documents from his supervisor's office. The documents were found in a closed desk drawer and contained notes and memoranda about sensitive personnel matters. Plaintiff was laid off a month later as part of a reduction in force and filed suit. During discovery, the defendant-employer learned of plaintiff's misconduct, and converted the layoff to a termination. Defendant successfully moved for summary judgment, arguing that the plaintiff's self-help discovery immunized it from any liability for discrimination in violation of the Age Discrimination in Employment Act (ADEA). Plaintiff countered "that by gathering evidence for an eventual lawsuit, he was participating in the investigation of an unlawful employment practice under the ADEA, or at the very least opposing such a practice."[64] In affirming the grant of summary judgment on the ADEA claim for defendant, the appellate court rationalized the competing interests:

> 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

61 *Id.* at 726.

62 *Id.* (quoting *Niswander v. Cincinnati Ins. Co.*, 2007 U.S. Dist. LEXIS 28911 (N.D. Ohio Apr. 19, 2017)).

63 79 F.3d 756 (9th Cir. 1996).

64 *Id.* at 763.

> flaunt company rules or an invitation to dishonest behavior.[65]

Similarly, in *Tides v. The Boeing Company*,[66] the employees, two auditors, obtained confidential business information during the course of their audit work and became concerned that their employer was violating SOX auditing and financial reporting requirements. Eventually, they released some of their confidential information to a newspaper reporter, who published an article stating that failures of internal controls put the employer's SOX compliance at risk. The defendant-employer learned that the plaintiffs had been the source of the information in the article and fired them.

The U.S. Court of Appeals for the Ninth Circuit rejected the plaintiffs' argument that the release of confidential information that related to potential SOX violations to the media was protected under 18 U.S.C. § 1514A(a)(1). The court upheld the termination.

Unfortunately for employers, this trend has not continued unabated. In *Vannoy v. Celanese Corp.*,[67] the employee in this case retained over 1,600 Social Security numbers of defendant's current and former employees and other confidential information, which the plaintiff stated were sent to the Internal Revenue Service (IRS) in support of his IRS disclosure. As a result of the plaintiff's improper retention of sensitive documents, the employer suspended plaintiff without pay and later terminated his employment. The Department of Labor's Administrative Review Board (ARB) held that: (1) theft of confidential personal and corporate information may be protected activity, depending on the circumstances surrounding the theft; and (2) the SOX anti-retaliation provision protects employees who make disclosures to the IRS under the IRS Whistleblower Rewards Program.

In *Quinlan v. Curtiss-Wright Corp.*,[68] the plaintiff believed that her employer had discriminated

against her when it promoted a man she thought was less qualified than she and made him her supervisor. In an effort to prove that her suspicions were true and that defendant was engaged in widespread sex discrimination, plaintiff gathered documents (including confidential employee information) that were available to her in the ordinary course of her employment and turned copies over to an attorney. During discovery in her discrimination lawsuit, defendant learned that plaintiff had taken, and was continuing to take, copies of hundreds of documents it considered to be confidential. Following disclosure of one document that was particularly helpful to plaintiff's claim that she had been discriminated against when she was not selected for the promotion, defendant fired her. The letter terminating plaintiff from her employment accused her of breach of company policies and theft. Believing that defendant had fired her because of the prosecution of her discrimination claim, plaintiff added a retaliation claim to her pending lawsuit. Although during the jury instruction, the court told the jurors that the taking of the documents was improper and the employer could rightfully terminate an employee based on this breach of the confidentiality agreement, the court allowed the documents to be used in plaintiff's discrimination case.

65 *Id.* at 763-64.
66 644 F.3d 809 (9th Cir. 2011).
67 ARB Case No. 09-118 (Sept. 28, 2011).
68 8 A.3d 209 (N.J. 2010).

D. Bar sanctions for attorneys

A potential twist comes where an attorney—either as the plaintiff or acting on behalf of a client who is bringing suit against an employer—discloses an employer's confidential and privileged information. Because attorneys are under ethical obligations to maintain client confidences, questions arise as to the reach of these duties and whether bar associations will take active steps to sanction an attorney who violates these obligations in the midst of litigation.

The American Bar Association's (ABA) Model Rule of Professional Conduct 1.6 permits disclosure of client information if the disclosure is necessary "to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client." The prototypical case is where an attorney is seeking unpaid fees from a client. Where an attorney is the plaintiff in an employment case, however, the ABA has also provided additional latitude to the attorney. In Formal Opinion 01-424 (2001), the ABA found that a wrongful termination claim is a "claim" within the meaning of Model Rule 1.6. Therefore, courts in states that have adopted the precise language of Model Rule 1.6 have held that, because of this exception, the ethical rule regarding disclosure of confidential information is not violated even if disclosure of client confidences is necessary to bring the claim.

A handful of states, including California and New York, have adopted more restrictive ethical rules regarding the disclosure of client confidences. In these states, the ethical rule regarding client confidences is violated if such confidences are disclosed by in-house counsel in the course of litigating a whistleblower claim, unless in-house counsel can show that some other exception applies, such as the crime-fraud exception discussed above.

New York's more restrictive ethical rules, for example, have also swayed state courts to dismiss cases brought by in-house attorneys against their employer. In *Wise v. Consolidated Edison Co. of New York, Inc.*,[69] the state appellate court ordered an in-house counsel's wrongful termination complaint dismissed because the case would require disclosure of the employer's confidential information in violation of a state rule of professional conduct. In *State of New York ex rel. Danon v. Vanguard Group, Inc.*,[70] a New York trial court went one step further than just a dismissal. Because the plaintiff violated state ethical rules (including a New York County Law Association (NYCLA) 2013 opinion restricting attorneys from collecting whistleblower awards) by bringing a *qui tam* action alleging tax fraud while he was still employed as an in-house tax attorney, the court ordered the case dismissed and instructed that the plaintiff "may not proceed with, nor profit from, any disclosure of confidential information to bring this [*qui tam*] action."[71] The court further ordered that the plaintiff and his counsel were disqualified from this or any subsequent action based on the same facts.

Even in states with more restrictive ethical rules, the underlying statute at issue in the litigation may limit the possibility of bar disciplinary proceedings. For example, the SEC's attorney conduct rules, referred to as "Part 205" and applicable only to attorneys representing issuers and "appearing and practicing" before the Commission, preempt state ethics rules, including state rules with more restrictive disclosure exceptions such as New York's. The pertinent regulation, 17 C.F.R. § 205.6, states that "[a]n attorney who complies in good faith with the provisions of this part shall not be subject to discipline or otherwise liable under inconsistent standards imposed by any state or other United States jurisdiction where the attorney is admitted or practices." This provision, therefore, appears to protect an attorney from discipline by a state bar association for disclosing confidential client information.

69 723 N.Y.S.2d 462 (N.Y. App. Div. 2001).

70 2015 N.Y. Misc. LEXIS 4239 (N.Y. Sup. Ct. Nov. 16, 2015).

71 *Id.* at *36.

Not all is lost, however. The court in *United States ex rel. John Doe v. X Corp.*,[72] discussed at length above, expressly held that the FCA does not preempt applicable state law regarding the disclosure of client confidences, and, accordingly, "where an attorney's disclosure of client confidences is prohibited by state law in a given circumstance, *that attorney risks subjecting himself to corresponding state disciplinary proceedings* should he attempt to make the disclosure in a *qui tam* suit."[73] The court in that case was more than willing to accept that bar disciplinary proceedings could proceed against an attorney.

III. CONCLUSION

Most of the case law cited in this paper comes from federal district court decisions. The new federal statute that will have a significant impact on this area — the DTSA — is two years old and has generated only one decision in the whistleblower area. However, based on prior law and current trends, employers should take note of a few general principles.

First, an employer whose departing employee has taken commercially valuable information like trade secrets has legal remedies and will likely be able to protect that commercially valuable information. A legally compliant confidentiality agreement will assist in that effort. It is more likely than ever that an employee who steals information will be prosecuted.

Second, an employer will not likely be able to protect information that could be proof of a crime from disclosure to law enforcement authorities, although the employer should be able to restrict dissemination of the information to the general public.

Third, courts continue to look askance at a lawyer's use of confidential information for attorney-client communications against the lawyer's former client, notwithstanding the result in *Wadler v. Bio-Rad Corp*.

Fourth, whether an employer can terminate an employee for stealing documents to use against the employer in a single plaintiff employment case is an open question that may turn on whether the employee has committed an unlawful act in order to obtain the documents. Employers should move carefully in this area and seek legal counsel before a termination.

72 862 F. Supp. 1502 (E.D. Va. 1994).

73 *Id.* at 1507 (emphasis added).


Littler
Employment & Labor Law Solutions Worldwide®