Originally published in the NJSBA Business Law Section Newsletter Vol. 39, No.1/October 2015

Protecting Confidential Information and Trade Secrets from Employee Theft in the Digital Age

by Martin W. Aron and Allison J. Vogel

In the Digital Age, companies face new and expanding legal and technological challenges. Employees regularly have access to sensitive technical, marketing, financial, sales or other confidential business information; trade secrets; and private or confidential personal information during their employment. Moreover, with ubiquitous social media and increasingly versatile personal devices that can record and broadcast through the Internet, it has become easier than ever for confidential information and trade secrets to fall into the hands of a disgruntled employee, with severely damaging consequences.

This article is intended to address the challenges of protecting confidential information and trade secrets from employee theft in light of recent case law developments. Companies can and should take affirmative steps to protect confidential information and trade secrets in order to protect valuable corporate assets and maximize the ability to obtain protection from the courts when necessary. This article discusses the type of information that is protected, the legal implications of an employee's unauthorized taking of confidential information from an employer and the employer's remedies. This article also discusses policies employers can implement to protect their confidential information and trade secrets.

Confidential Information and Trade Secrets

In Jan. 2012, New Jersey enacted a version of the Uniform Trade Secrets Act (UTSA), entitled the New Jersey Trade Secrets Act (NJTSA), to protect trade secrets.[1] The NJTSA defines a "trade secret" as information, held by one or more people, without regard to form, including a formula, pattern, business data compilation, program, device, method, technique, design, diagram, drawing, invention, plan, procedure, prototype or process, that:

***

> (1) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and
>
> (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[2]

***

The NJTSA further defines "misappropriation" as "(1) [a]cquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means"; or "(2) [d]isclosure or use of a trade secret of another without express or implied consent of the trade secret owner by a person who: (a) used improper means to acquire knowledge of the trade secret; or (b) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was derived or acquired through improper means; or (c) before a material change of position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired through improper means."[3]

Under the NJTSA, employers must ensure their trade secrets are "the subject of efforts that are reasonable under the circumstances to maintain [their] secrecy."[4] Such efforts may include limiting disclosure of confidential information and trade secrets within the company, implementing security measures to restrict the manner in which confidential information is stored or maintained, requiring employees in any sensitive position to sign confidentiality agreements, and monitoring the effectiveness of security measures electronically. Senior management, sales, marketing and financial personnel, and technical and production employees, such as chemists and engineers, should be required to execute a confidentiality, non-solicitation and non-disclosure agreement to protect the company's interests.

Such agreements typically cover, at a minimum, an appropriate definition of the confidential information or trade secrets to be protected, confirmation of the requirement to return such information and all copies upon termination, assignment of rights in any inventions, confirmation of at-will status, post-employment covenants not to solicit other workers upon termination, and agreement to the appropriateness of injunctive relief in the event there is a breach or threatened breach of the agreement. The agreement also can address choice of law and venue options to best suit the company's interests in the event of litigation. Any such agreement should conform with other company policies, such as those that might be contained in an employee handbook.

Unauthorized Taking of Confidential Documents to Support Employment Claims

Despite the existence of comprehensive agreements, employees may nonetheless attempt to obtain and remove confidential information without authorization in order to obtain a position with a competitor, gain a competitive advantage in the marketplace, or pursue legal action against the employer. The NJTSA provides for broad equitable and legal relief in addition to reimbursement of counsel fees for a misappropriation of trade secrets.[5] In addition, there are a number of statutes that can be implicated when electronically stored information is stolen by employees. Under the New Jersey Computer-Related Offense Act (CROA), a person may be liable if he or she purposefully or knowingly, and without authorization, takes data existing on a computer, computer system or computer network.[6] Likewise, the federal Computer Fraud and Abuse Act (CFAA) prohibits the unauthorized access, or the exceeding of authorized access, to computers.[7]

While an employer has a legitimate right to safeguard its confidential documents and trade secrets, recent case law has shown that this right is not absolute. In 2010, the New Jersey Supreme Court had occasion to develop a framework for courts to use to determine whether an employee's removal of confidential documents from her employer's files in the context of prosecuting a discrimination case is protected conduct under the New Jersey Law Against Discrimination (LAD).[8]

Joyce Quinlan was employed as an executive director of human resources in Curtis-Wright Corporation's human resources department. In 2003, the company promoted a male employee to the position of corporate director of human resources and management development, which made him Quinlan's supervisor. Quinlan believed the male employee was less qualified than her. In order to prove her allegation that her employer discriminated against her and engaged in widespread gender discrimination, Quinlan gathered over 1,800 pages of internal documents from her employer's confidential files, including confidential personnel files, and provided them to her attorneys.

In Nov. 2003, Quinlan filed a lawsuit against her employer alleging gender discrimination. During discovery, Quinlan's attorneys produced the 1,800 pages of documents Quinlan had turned over to them. Shortly thereafter, Quinlan came into possession of her supervisor's performance review in her capacity as executive director of human resources. She copied the document and provided it to her attorneys, who used it during her supervisor's deposition. Once the company became aware of Quinlan's unauthorized removal of confidential and privileged information, it terminated her for theft of company property. Following her termination, Quinlan amended her complaint to add a claim for retaliation.

The first jury trial ended in a mistrial and the second jury trial resulted in a substantial compensatory and punitive damages award in the plaintiff's favor.[9] On appeal, the Appellate Division reversed and remanded the retaliation verdict for a new trial, and vacated the punitive damages award.[10] The plaintiff petitioned the New Jersey Supreme Court for certification.

The Supreme Court began its analysis of the employee's removal of documents by recognizing that "employees have a common law duty to safeguard confidential information they have learned through their employment relationship and that they are generally precluded from sharing that information with unauthorized third parties."[11] The issue, however, required the Court to "strike the balance between the employer's legitimate right to conduct its business, including its right to safeguard its confidential documents, and the employee's right to be free from discrimination or retaliation."[12]

The Court found that the following factors should be considered in deciding whether an employee is privileged to take or use documents belonging to the employer: 1) how the employee obtained possession or access of the documents; 2) what the employee did with the documents; 3) the nature and content of the documents; 4) whether the company had a clearly identified privacy or confidentiality policy; 5) whether disclosure of the documents was unduly disruptive to the employer's ordinary business; 6) the strength of the employee's expressed reasons for copying the documents; and 7) the impact of the broad remedial purposes of anti-discrimination laws and the balance of employer and employee rights.[13]

Importantly, the Court asserted it was "mindful that employers may fear that [it had] opened the floodgates by granting protected status to such conduct," but it "[did] not share the concern that employers will be powerless to discipline employees who take documents when they are not privileged to do so."[14] Rather, the Court made it clear that "employees may still be disciplined for that behavior and even under the best of circumstances, run the significant risk that the conduct in which they engage will not be found by a court to fall within the protection [the court's] test creates."[15]

Applying these standards, the Supreme Court found Quinlan's act of removing the documents, including her supervisor's performance review, was not protected activity, and her employer could terminate her for her actions.[16] The Court also found the jury was correctly instructed to decide whether the company actually terminated Quinlan for taking the documents or for pursuing her claim that the failure to promote her was discriminatory. Given that the jury was correctly instructed at the trial court level, the Supreme Court reversed the judgment of the Appellate Division and reinstated the retaliation verdict.[17]

Prosecuting Employees for Unauthorized Taking of Confidential Documents

While *Quinlan* may have granted protected status to an employee's unauthorized taking of confidential documents in the context of prosecuting a discrimination case, such action may now be at the employee's own peril.[18] More recently, the Supreme Court addressed the criminal

prosecution of an employee for unlawfully taking highly confidential documents obtained during the course of an employment relationship to support employment claims.[19]

Ivonne Saavedra was employed by the North Bergen Board of Education. In 2009, Saavedra and her son filed a lawsuit against the board alleging claims of employment discrimination and retaliation under the LAD, the Conscientious Employee Protection Act (CEPA), and other state and federal statutes. At some point, Saavedra gathered over 367 confidential student records, including 69 original file copies, without her employer's permission, to use in support of her discrimination lawsuit. Saavedra's counsel produced copies of the records in response to the board's discovery requests.

Upon learning that Saavedra removed the board's confidential documents, the board's counsel notified the county prosecutor's office. The county prosecutor pursued charges against Saavedra and presented evidence to a grand jury. The grand jury returned a two-count indictment charging Saavedra with second-degree official misconduct and third-degree theft by unlawful taking of public documents. Following her indictment, Saavedra voluntarily dismissed her employment discrimination lawsuit against the board.

She moved to dismiss the indictment, which was denied by the trial court. On appeal, the Appellate Division affirmed the trial court's denial of Saavedra's motion to dismiss the indictment.[20] She petitioned the New Jersey Supreme Court for certification, asserting, in part, that the Appellate Division's decision should be reversed because it "contravenes the anti-discrimination policies of the LAD, CEPA, and the Supreme Court's decision in *Quinlan*, and that it authorizes employers to circumvent the *Quinlan* balancing test by reporting an employee's collection of documents as a theft to a prosecutor."[21]

The Supreme Court found the "court rules provided [Saavedra] the opportunity to obtain from the Board relevant documents in support of her civil claim, subject to procedural safeguards and judicial oversight."[22] Contrary to Saavedra's assertion, the Court found its decision in *Quinlan* "did not endorse self-help as an alternative to the legal process in employment discrimination litigation" or "bar prosecutions arising from an employee's removal of documents from an employer's files for use in a discrimination case, or otherwise address any issue of criminal law."[23]

The Court revisited its analysis in *Quinlan* and found the balancing test may be used in cases involving retaliation under the LAD "when the employee's conduct in taking or using confidential documents allegedly provoked the employer to take retaliatory action."[24] The Court also reiterated that "nothing in *Quinlan* state[d] or implie[d] that the anti-discrimination policy of the LAD immunizes from prosecution an employee who takes his or her employer's documents for use in a discrimination case."[25] The Court, therefore, concurred with the Appellate Division that the statutes met due process standards.[26] Accordingly, the Court affirmed the judgment of the Appellate Division and remanded the matter to the trial court.[27]

Company Policies and Handbooks

It is prudent for employers to implement policies to protect their confidential information and trade secrets. The New Jersey Supreme Court suggested that courts consider whether a company has a clearly identified privacy or confidentiality policy that the employee's disclosure violated as a factor in deciding whether an employee is privileged to take or use documents belonging to the employer. By implementing confidentiality and privacy policies, codes of business conduct and ethics, and including confidentiality and privacy policies in employee

handbooks, employers place their employees on notice that the unauthorized taking of confidential documents constitutes theft and can result in an employee's termination.

Employers also may require employees to sign post-employment agreements with restrictive covenants concerning the disclosure of confidential information. Such agreements ensure the company's confidential information and trade secrets remain protected during and for a specified period of time after the employee's separation with the company.

Employers also may consider implementing an electronic communications policy. By implementing an electronic communications policy, a company can identify permissible and impermissible uses of the company's systems, email, and Internet access. Companies also can restrict their employees' personal usage of information systems and monitor employees' business and personal communications to protect their confidential information and trade secrets.

Employers may consider instituting a 'bring your own device' (BYOD) program in recognition of the rapidly emerging technology and devices used for personal and other communications. A BYOD program permits eligible employees and certain others limited connectivity to the company's corporate networks. The purpose of a BYOD policy is to define standards, procedures, and restrictions governing participation in the program for individuals who wish to connect a mobile personal device.

Finally, employers can request employees sign acknowledgements stating that non-compliance with the terms and conditions of the program and policies will subject them to disciplinary action, up to and including termination of access to the company's information systems or disciplinary action, including termination of employment or association with the company. An employer will stand on stronger ground in court if it can prove the employee was on notice and aware of the company's policies.

Conclusion

Employers must take affirmative steps to protect confidential information and trade secrets. Failure to do so could cause a court to question whether the information warrants the issuance of injunctive relief. Confidentiality agreements and corporate policies must place individuals on notice of the consequences of improper use or removal of such information. In light of the *Saavedra* decision, employees also are on notice that they may be subject to criminal prosecution for unlawfully taking confidential documents. While the legal landscape continues to develop with new technologies, companies must ensure they constantly review and monitor the measures that are in place for protecting valuable intellectual property and trade secrets that are vital to business operations.

Martin W. Aron *is a shareholder and litigation manager in the Morristown office of Jackson Lewis P.C.* ***Allison J. Vogel*** *is an associate of the firm.*

Endnotes

1. N.J.S.A. 56:15-1, *et seq.*
2. *Id.* 56:15-2.
3. *Id.*
4. *Id.*
5. N.J.S.A. 56:15-3 and 56:15-4.
6. N.J.S.A. 2A:38A-3.
7. 18 U.S.C.S. § 1030.

8. *Quinlan v. Curtis-Wright Corp.*, 204 N.J. 239 (2010).
9. *Id.* at 244.
10. *Id.*
11. *Id.* at 260.
12. *Id.* at 261.
13. *Id.* at 269-71.
14. *Id.* at 272.
15. *Id.*
16. *Id.* at 273.
17. *Id.*
18. For example, in *West Hills Research and Development, Inc.*, 2015 Cal. App. Unpub. LEXIS 5009 (Cal. Ct. App. 2d Dist. July 17, 2015), the court held that a former employee's taking of his former employer's confidential information in order to prepare for filing a shareholder derivative lawsuit was not protected activity under California's Anti-SLAPP statute.
19. *State v. Saavedra*, 2015 N.J. LEXIS 641 (S. Ct. June 23, 2015).
20. *State v. Saavedra*, 433 N.J. Super. 501 (App. Div. 2013).
21. *Saavedra*, 2015 N.J. LEXIS 641, at *23.
22. *Id.* at 50.
23. *Id.*
24. *Id.* at 54.
25. *Id.*
26. *Id.* at 55.
27. *Id.* at 61.