PLAN YOUR DEPARTURE CAREFULLY: THE ARSENAL OF REMEDIES AGAINST DISLOYAL EMPLOYEES IN NEW JERSEY

By Kevin J. O'Connor*

A decision this week from the New Jersey Appellate Division, B&H Securities, Inc. v. Pinkney, A-3741-12T1 (App. Div. Apr. 28, 2015) illustrates just how broad an arsenal of legal relief is available to bring to bear against a disloyal employee, and the reason why departing employees should always seek legal counsel to steer clear of such legal action. The Court affirmed the rationale for a seven figure judgment against disloyal employees and their new company, remanding only for the trial court to explain limited parts of its holding.

In B&H, the employer is in the business of designing, selling, installing and maintaining security systems for its clients. Its business is primarily in New Jersey but it operates in thirteen other states. It regards the names and identifies of its clients, as well as the particulars of each client's needs, as confidential, as well as various business materials entrusted to the defendant employees. B&H maintained a handbook which included a confidentiality clause that it asks its employees to acknowledge. B&H maintained confidential information on its servers to which the employees also had access.

In early 2007, several B&H employees (Pinkney, Palladino and Poisler) formed a plan to start their own security business. They created an operating agreement for a new entity. They formed an agreement with B&H's information technology employee to help them in this endeavor with a promise of financial remuneration. The evidence at trial showed that they actively solicited clients of B&H before they departed. For some clients, they arranged for new contracts allowing services to be terminated on shorter notice. The evidence also showed that these departing employees accessed information on B&H's servers to use in their new business, and spoliated evidence by wiping a computer clean with a program designed for that purpose.

The employer sued the departed employees on a number of theories and the result was predictable, although it obviously took a great deal of time and money to get to the end. B&H sued the employees on common law and statutory theories, including claims for breach of duty of loyalty, breach of the implied covenant of good faith and fair dealing, and violation of the New Jersey Computer Related Offenses Act ("NJCROA"). An attempt by certain of the defendants to thwart the claims through a bankruptcy filing was not effective and the case proceeded with leave of the bankruptcy court.

This decision is significant in several respects. First, the Court ruled that Defendant Poisler could be held liable on a theory of breach of the implied covenant of good faith and fair dealing, which claim stemmed simply from the at will employment relationship rather than an acknowledgment to the confidentiality provisions in the company's handbook. Poisler had argued that well-established New Jersey precedents recognize that a disclaimer in a company handbook that it does not constitute a contract prohibits a court from finding contract rights stemming from that handbook. Accordingly, he argued, there could be no breach of implied covenant claim stemming from his acknowledgment of the handbook confidentiality provisions. The Court ruled that Poisler had an "agreement" with the company to work for it, which was undisputed, and that the covenant not to do all of things he did was "an implied term of that agreement" which was violated. Slip Op. at 12.

Since the evidence of unfair competition was so clear, its not at all clear why this theory was needed, but the Court's holding in this regard could be applied in different contexts and is significant. Essentially, the Court found the existence of an implied covenant of good faith and fair dealing in the at will employment relationship itself.

The second part of this opinion which is of significance is the Court's holding that the NJCROA, N.J.S.A. § 2A:38A-3 *et. seq.* is violated by exceeding authorized access to computers. Cases interpreting the NJCROA are few and far between. With the proliferation of technology in the modern workplace, employee theft of confidential, proprietary and secret computer data is becoming commonplace, and we can expect to see more of these cases. The NJCROA is an often overlooked, potent remedy for employers that can provide relief even where the federal counterpart, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq. ("CFAA") might not apply.

The CFAA, a federal act, provides a private right of action to those who have suffered "losses" due to violations of the Act. See 18 U.S.C. § 1030(g). Section 1030(a)(2)(c) imposes liability, among other things, upon any person who intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from a protected computer. Under the CFAA, a "protected computer" is one which, among other things, is used in interstate commerce or communication. 18 U.S.C. § 1030(e)(2)(B).

The Third Circuit in P.C. Yonkers, Inc. v. Celebrations: The Party and Seasonal Superstore, LLC, 428 F.3d 504, 510-511 (3d Cir. 2005), recognized the availability of injunctive relief under the CFAA, but expressly held that an employer must show more than mere unauthorized access to a computer, and must make a specific showing of a probability of success on each of the elements of its claim. Id. at 509.

For its part, the NJCROA provides that a person or enterprise damaged in its business or property may recover compensatory and punitive damages and the cost of the suit, including attorney's fees, costs of investigation and litigation, where an employer can establish computer-related misconduct. Fairway Dodge, LLC v. Decker Dodge, Inc., 191 N.J. 460, 468-69 (2007).

For instance, liability under the NJCROA "is established if an actor, purposefully or knowingly and without authorization, accesses or attempts to access, any computer system or computer network, or if an actor purposefully or knowingly accesses and recklessly obtains any data." Fairway Dodge, Inc. v. Decker Dodge, Inc., 2005 WL 4077532 at *10 (N.J. App. Div. June 12, 2006), rev'd on other grounds, 191 N.J. 460 (2007).

The NJCROA has been interpreted as providing that an employee who accesses his employer's computer for competitive purposes cannot contend under the NJCROA that his actions were "authorized." Fairway Dodge, 2005 WL 4077532 at *9-12. Similarly, a defendant cannot avoid liability under the NJCROA by contending that he or she merely "copied" documents, as opposed to deleting or altering them. Id. The federal courts have not universally interpreted the CFAA in the same manner, however, largely because of a general reluctance to create a private right of action under a federal statute for simple common law misappropriation.

B&H also clarified that an employee who prepares for his departure may be found in violation of the duty of loyalty if he crosses the line, which the Court found had clearly been crossed in the case before it Performing work for a competitor before your departure is problematic and dangerous. Speaking to clients about moving over, before departure, is equally problematic.

In the end, the Appellate Division affirmed much of the award below, but remanded for the trial court to explain the rationale for its damage award against Poisler given that he had left the competing firm during the litigation and disassociated himself. B&H shows the breadth of legal remedies available to employers against departing employees, and the need for departing employees to carefully plan their exit so as not to violate any written contract with the employer or prohibitions under statutory or common law.

*Kevin J. O'Connor, Esq. is a shareholder with Peckar & Abramson, PC, a national law firm, and focuses his practice on EPLI , D&O, and class action defense. He is resident in P&A's River Edge, NJ office. The views expressed herein are those of the author and not P&A.