New Jersey Law Journal

VOL. 214 - NO 11 MONDAY, DECEMBER 16, 2013 ESTABLISHED 1878

IN PRACTICE

EMPLOYMENT LAW

Computer Related Offenses Act Protects Against Theft of ESI

New Jersey's statute provides a powerful tool for employers

By Rosaria A. Suriano, Melissa A. Clarke and Eric Holmes

Technology has simplified access to electronically stored information. Today, thousands of pages of data can be copied and transferred onto an inexpensive thumb drive or other computer device. As a result, information such as pricing, pricing strategies and methods, customer or client information, and even proprietary designs and formulas, can be downloaded and forwarded to a personal email address or another computer network with a few clicks of a mouse. Proprietary information that may have taken years to develop at significant cost will be at risk, along with a company's competitive advantage. Intrusion into computer data can be ascertained and, in many instances, an intruder identified, with the aid of a forensic computer expert, albeit at significant expense. This article will address the relief available to an employer facing employee theft of electronically stored computer data.

Suriano is a partner with Meyner and Landis in Newark and represents companies in business disputes, commercial litigation, noncompete agreements and business-related claims. Clarke and Holmes are associates with the firm.

Common-Law Remedies

A variety of common-law remedies exist that can address employee theft or misuse of computer information. These include (but are not limited to): misappropriation of trade secrets or confidential information; tortious interference with prospective economic advantage; and breach of contract claims, including a breach of duty of loyalty to the employer. Though common-law remedies are abundant, the level of proof required may be onerous. For instance, to succeed on a claim of misappropriation of a trade secret, an employer must first prove that the information qualifies as a "trade secret" and that the "trade secret" was misappropriated, i.e., the information comprising the trade secret was communicated in confidence by employer to employee; the secret information was disclosed by that employee and in breach of that confidence; the secret information was acquired by a competitor with knowledge of the employee's breach of confidence; the secret information was used by the competitor to the detriment of plaintiff; and the plaintiff took precautions to maintain the secrecy of the trade secret. *Rycoline Products v. Walsh*, 334 N.J. Super. 62, 71 (App. Div. 2000).

N.J. Computer Related Offenses Act

The New Jersey Computer Related Offenses Act, N.J.S.A. 2A:38A-1 et seq. ("Computer Act"), provides a statutory remedy for the wrongful access or misuse of computer data. The act specifically protects against the "taking" of "any data" and creates a private right of action against an "actor" who purposely or knowingly accesses, alters, damages, takes or destroys computer information. N.J.S.A. 2A:38A-3. Importantly, the Computer Act prohibits the taking of *any* data contained on a computer system; it is not limited to proprietary or confidential information. However, in order to impose liability under the Computer Act, there must be "proof of some activity vis-à-vis the information other than simply gaining access to it." *P.C. Yonkers v. Celebrations the Party & Seasonal Superstore*, 428 F.3d 504, 509 (3d Cir. 2005).

Damages Under the Act

Damages available under the Computer Act include "compensatory and punitive damages and the cost of the lawsuit including reasonable attorney's fees, costs of investigation and litigation." N.J.S.A. 2A:38A-3. This provides a significant benefit to the employer bringing a Computer Act claim. Unless there is a fee-shifting agreement, attorney fees may not otherwise be recoverable under common-law tort or breach-of-contract claims. Moreover, the potential to recover investigative and litigation costs may motivate the employer to proceed with expensive forensic investigation into an employee's intrusion or misuse of data, and with a lawsuit where litigation costs may have otherwise impeded such action. The ability to recover punitive damages is an additional benefit to bringing a claim under

the Computer Act. Because the act does not specify the standard applicable to an award of punitive damages, the court has applied the standard set forth in the Punitive Damages Act, N.J.S.A. 2A:15-5.9 to -5.17; that is, clear and convincing evidence that defendants acted either with actual malice or with wanton and willful disregard. *Fairway Dodge v. Decker Dodge*, 2005 WL 4077532, at *20 (App. Div. June 12, 2006), aff'd sub nom., *Fairway Dodge, v. Decker Dodge*, 191 N.J. 460 (2007).

Injunctive Relief

The Computer Act expressly provides that a "person or enterprise alleging injury or loss may bring an action in Superior Court to enjoin actions causing damage…or to enjoin any acts in furtherance thereof." N.J.S.A. 2A:38A-5. Injunctive relief is essential in limiting or eliminating the employee's ability to copy and transfer electronic data which may be virtually impossible to trace and retrieve. To obtain an injunction, the movant must meet the requirements set forth in *Crowe v. DeGioia*, 90 N.J. 126, 132–34 (1982). An order requiring the employee to delete information from a new employer's computer system and to refrain from soliciting a former employer's customers is the type of injunctive relief available in a Computer Act case, and which actually was utilized in *Fairway Dodge*. In addition, it is possible that the relief granted may include access to the new employer's computer network to ascertain whether and what data has been transferred.

Fairway Dodge involved two competitor car dealerships and is the only published decision addressing a Computer Act claim. Fairway Dodge, the plaintiff and former employer, initially instituted an action in the Chancery Division, seeking injunctive relief and damages after learning that the information in its computer system had been copied by the defendants—former Fairway employees—and taken to their new employer, the defendant Decker Dodge. The trial judge granted the application and ordered the defendants to show cause why they should not be enjoined from using the information or from soliciting Fairway's customers. Subsequently, a consent order was entered whereby the defendants agreed to: (1) make a copy of the "backup" data in Decker's system; (2) arrange for the deletion of the stolen information from Decker's system; (3) make another backup tape of the system after the deletion; and (4) refrain from soliciting customers from lists generated from the backup tape. The defendants further agreed to certify that they did not possess any other copy of customer lists originated by Fairway and had neither delivered this information to any other person nor altered the data.

An injunction is difficult to enforce when dealing with something as intangible as computer data. Thus, the injunction should require the defendants to provide a "before and after" copy of their computer system, and certifications regarding possession and use of information. Even so, the possibility remains that a defendant may use previously obtained computer data, such as customer lists, in violation of the temporary injunction, as was the case in *Fairway Dodge*.

The New Employer's Liability

Fairway Dodge also provides guidance regarding who can be responsible for "taking" or for the "unauthorized use" of computer data under the Computer Act. As discussed above, Fairway sued Decker, two of its principals and two departing employees after an investigation revealed that Fairway's entire computer system had been copied by those departing employees. Decker's principals argued that since they did not actually access Fairway's computer system, they were not liable under the Computer Act because they were not "actors." The Appellate Division concluded that the meaning of the word "actor" was crucial and declared that the "only parties liable pursuant to the [Computer Act] are those actors that actually access, alter, damage, take or destroy computer information." The Supreme Court found that Decker's owners lacked the specific intent required by the Computer Act to hold the owners personally liable for the departing employees' actions. However, the court upheld the Appellate Division's decision that the new employer may, like Decker, be liable under respondeat superior, provided the plaintiff can establish that the departing employee committed the computer offense *after* accepting a position with the new employer. In so holding, the court declined to define the word "actor," so this remains an open issue.

Fairway Dodge also provides guidance regarding an employee's authorization to access electronic data. In response to the defendant's argument that he was still an employee when the electronic data copying occurred and was thus authorized to access the information, the Appellate Division expressly held that "status as a mere employee" does not confer such authorization. Employers should still identify what is permissible access during employment and clarify that employee computer access ceases upon termination of employment.

Criminal Component

New Jersey has also provided criminal penalties, at N.J.S.A. 2C:20-25, for certain computer-related conduct that is more egregious than what is covered by the Computer Act. Violations of the criminal statute range from fourth-degree to first-degree crimes, depending on the section violated, the value of the data, database, computer program, computer software or information, and the severity of the results of the violation. A company can initiate a criminal investigation by reporting the alleged violation to the Division of Criminal Justice and the State Police.

The Computer Act provides a powerful remedy to a company that has had computer data, programs, applications, systems and/or equipment wrongfully and without authorization accessed, altered, taken or destroyed. Given the continuing advancement of technology, the Computer Act's necessity and applicability are likely to increase. The ability to obtain compensatory and punitive damages, as well as the costs of suit, reasonable attorney fees and costs of investigation are enormous benefits to a plaintiff bringing a claim under the Computer Act. However, there are only a handful of cases that address the Computer Act, only one of which is published, and the meaning of the term "actor" remains subject to debate. ■