New Jersey Law Journal

VOL. 211 - NO 5 FEBRUARY 4, 2013 ESTABLISHED 1878

IN PRACTICE

TORTS

Modern Solution to the Timeless Problem of Stolen Data

A fresh look at the Computer Related Offenses Act

By Ronald L. Israel, Marie L. Mathews and Brian P. O'Neill

As many companies have learned, a paperless workplace is often a vulnerable workplace — perpetrating information piracy has never been easier. This development directly impacts commercial litigation, which increasingly involves disputes over information stored on digital platforms. The fundamental principles of business litigation will survive the transition to a more technology-based work environment; a well-guarded proprietary formula enjoys protection whether stored in a cabinet or on a hard drive. Still, the modern litigator should not rely solely on case law involving stolen rolodexes or Redwelds. Indeed, as businesses evolve, their lawyers must, too.

To that end, New Jersey practitioners should familiarize themselves with the state's Computer Related Offenses Act (CROA), N.J.S.A. 2A:38A-1 to -6. Enacted in 1984, CROA provides a civil remedy to businesses and individuals "damaged in business or property" as a result of "[t]he purposeful or knowing, and unauthorized accessing or attempt to access any computer, computer system, or computer network." N.J.S.A.2A:38-3(c). The law similarly applies to intentional "and unauthorized altering, damaging, taking or destruction of any data." N.J.S.A. 2A:38-3(e). Liability is imposed on the "actor," an undefined term.

Thus far, CROA claims have targeted only misappropriations of information — a form of wrongdoing that has regularly appeared in commercial litigation for the past century. A seemingly unending list of causes of action already exists to address every variation of misappropriation: theft of trade secrets, misappropriation of confidential information, tortious interference, breach of the duty of loyalty, trespass to chattel, and so on. The many alternatives are no secret to commercial litigators.

Why, then, is CROA important?

First, successful CROA claimants "may recover compensatory and punitive damages and the cost of suit *including a reasonable attorney's fee, costs of investigation and litigation*." N.J.S.A. 2A:38A-3. This provision is quite formidable because common-law business torts hold little or no prospect of returning attorney fees unless the parties have contractually agreed to shift fees. Attorneys should also note that investigative costs are recoverable in addition to counsel fees. Many businesses may strongly suspect that computer tampering has occurred but refrain from investigating because of the attendant costs. CROA addresses this issue by permitting a successful claimant to recover the costs expended in determining whether its computer system was in fact compromised.

Second, CROA applies to "*any* data" accessed without authorization. The language plainly suggests that, at least with respect to liability, claims need not involve trade secrets or otherwise confidential and proprietary information. Indeed, the Appellate Division confirmed that CROA's "sweep is not limited to proprietary or confidential information," and that the law "concerns any data contained on a computer system." *Fairway Dodge v. Decker Dodge*, A-1736-03T2, 2005 WL 4077532, at *10 (App. Div. June 12, 2006), *aff'd*, 191 N.J. 460 (2007). Similarly, a New York trial court denied a motion to dismiss CROA claims against defendants that had misappropriated information owned by the plaintiff's clients and stored in the plaintiff's New Jersey office. See *A & G Research v. GC Metrics*, 19 Misc.3d 1136(A) (N.Y. Sup. Ct. 2008) (approving CROA's extraterritorial application). CROA thus appears to operate as a less stringent alternative to claims for theft of trade secrets and misappropriation of confidential information.

Case law involving CROA claims is remarkably scarce and includes only a single published New Jersey decision, *Fairway Dodge v. Decker Dodge*,

Israel is a member of Wolff & Samson PC in West Orange. Mathews and O'Neill are associates in the firm's litigation group.

191 N.J. 460 (2007), and a handful of unpublished decisions. The limited body of law is comprised entirely of two age-old fact patterns. The first category includes *Fairway Dodge* and similar cases in which an employee copies information from his employer's computer system and thereafter uses the information in a competing enterprise. See, e.g., *P.C. of Yonkers, Inc*., No. 04-4554, 2007 WL 708978 (D.N.J. Mar. 5, 2007). In the second category, businesses share proprietary information in furtherance of a service contract or joint venture, and one party exploits or continues to access that information after the relationship has ended. See, e.g., *Joseph Oat Holdings v. RCM Digesters*, 409 F. App'x 498, 503 (3d Cir. 2010). The most recent judicial decision to feature CROA claims falls within the first category. See *B&H Securities v. Pinkney*, No. UNN-L-1292-08 (Ch. Div. 2013). On Jan. 2, 2013, Judge Kessler awarded compensatory and punitive damages under CROA to B&H Securities, a company that sued three former employees and the competing company they established.

Fairway Dodge illustrates two issues that very often arise in CROA litigation. The case involved a fairly typical commercial dispute between competing car dealerships, Fairway Dodge and Decker Dodge. Soon after Decker hired two of Fairway's employees, Fairway's sales rapidly declined, and an investigation revealed that Fairway's entire computer system had been copied. Fairway sued Decker, two of its principals and the two employees.

The trial judge entered partial summary judgment on liability against Decker and the two employees. A jury then assessed CROA liability against all defendants but found that only Decker's and the employees' violations caused damage. To calculate damages, Fairway presented an accounting expert whose testimony was based on historic profit and overhead figures, goodwill valuations and assumptions regarding client retention.

The first major issue faced on appeal was whether liability could be imposed on defendants who had not personally accessed any data. Decker and its principals argued that they were not "actors" under CROA because, unlike like the transitioned employees, they did not actually access Fairway's system. The Appellate Division agreed with respect to the principals and held that CROA applies only to "those actors that actually access, alter, damage, take or destroy computer information." Decker, however, remained liable under respondeat superior because one of the employees had already accepted Decker's offer of employment when the misconduct occurred.

The Supreme Court affirmed the Appellate Division's decision but on different grounds. Specifically, the court found that Decker's principals lacked specific intent, a requirement under CROA. Resting on these grounds, the court explicitly avoided defining "actor," which remains undefined. Consequently, CROA's limits are still subject to debate. See *A & G Research*, 19 Misc.3d 1136(A) (holding that two business partners and their corporation, formed after the misappropriation, could be liable when a third partner copied confidential information from his employer's New Jersey office).

The second major issue relates to the actor's authority to access the data. On the day the two employees accessed and copied Fairway's system, one of the employees had already joined Decker but remained Fairway's corporate secretary. On appeal, the panel flatly rejected the notion that her lingering officer status provided authority to access Fairway's system. The second employee, however, offered a more compelling argument that CROA defendants frequently raise. He was still an employee when the copying occurred, and thus, he argued, his access was authorized. The Appellate Division disagreed, holding that "his status as a mere employee did not give him such authorization." Nonetheless, attorneys should advise their clients to clearly communicate to former business partners or employees that computer access is no longer authorized as some courts are unwilling to assume that authority ends with the relationship. See *Joseph Oat Holdings*, 409 F. App'x at 505.

While some may argue that the newly enacted New Jersey Trade Secret Act (NJTSA), N.J.S.A. 56:15-1 to -9, pre-empts other causes of action based on misappropriation, this position was recently rejected in the Chancery Division. See *SCS Healthcare Marketing v. Alleran, USA*, No. C-268-12 (Ch. Div. Dec. 7, 2012). In drafting the NJTSA, New Jersey's legislature largely adopted the Uniform Trade Secrets Act (UTSA). Judge Carroll's decision in *SCS Healthcare* notes that the majority of states with UTSA-based legislation have interpreted the law to "abolish all free-standing alternative causes of action for theft or misuse of confidential, propriety, or otherwise secret information." The Chancery Division, however, pointed to a unique clause in the NJTSA that does not appear in other states' trade secret laws: "[t]he rights, remedies and prohibitions provided under this act are in addition to and cumulative of any other right, remedy or prohibition provided under common law or statutory law of this State." N.J.S.A. 56:15-9. After lamenting that "the statute is not the model of clarity," the court concluded that the NJTSA permits the continued assertion of misappropriation claims.

The authors believe that the opportunity for companies to assert CROA claims will rise steadily as technology simplifies access to confidential information. In the 2008 *A & G* case cited above, the A & G employee explained how she brought home almost 6,000 confidential files: "I simply plugged (the portable hard drive) into the USB port on my computer (at A & G) and a little screen popped up, said, what do you want to do. I pointed ... and just click[ed] on it, and that was it." Plaintiff's attorneys should thus consider alleging a cause of action under CROA for any misappropriation case involving electronic data. ■