New Jersey Law Journal

VOL. 201 - NO 9 AUGUST 30, 2010 ESTABLISHED 1878

IN PRACTICE

EMPLOYMENT LAW

A Rarely Used Weapon for Employers: The Computer Related Offenses Act

BY RODMAN E. HONECKER

The explosion of information technology has brought much efficiency to employers but also many challenges. Important company data of every kind is easily accessible to a broad range of employees. Financial and customer data, sales and sales leads information, are only the most obvious. By pushing a few buttons, that data can easily be downloaded and forwarded to separate systems. Serious loss of competitive advantage can occur in the blink of an eye.

The good news for employers is that incursions into company data leave footprints that can be traced. Investigation of systems, computer hard drives and network server history will reveal a detailed record of any data accessed, forwarded or deleted. Most likely, the individual responsible will also be easily identified.

But armed with proof positive of data theft, what can an employer really do to right the wrong after the fact?

Employers and companies should be mindful of their rights to protect company data and information against unauthorized access and misappropriation by employees, former employees and competitors. New Jersey's Computer Related Offenses Act, N.J.S.A. 2A:38A-1, et seq. ("CROA"), provides a broad array of private causes of action and remedies. Although CROA was enacted over 25 years ago, very few opinions have been published interpreting the statute, suggesting a general lack of familiarity regarding this potentially potent statute.

CROA provides a private cause of action to any person or company damaged by knowing and unauthorized accessing, damaging or taking of company data. "Data" is broadly defined to include "information, facts, concepts, or instructions prepared for use in a computer, computer system, or computer network." "Data" is not limited to proprietary or confidential information. A purposeful and reckless accessing of a computer system resulting in damage to the computer software, equipment or network is also covered.

The remedies offered by CROA run the gamut. Compensatory and punitive damages are available. Reimbursement of attorneys' fees and costs are also available, as well as costs of investigation. This includes, of course, forensic IT investigative expenses. Injunctions are also expressly provided for in the statute.

A common scenario involves misappropriation of company data by employees who go on to work for competitors. In *Fairway Dodge, L.L.C. v. Decker Dodge, Inc.*, 191 N.J. 460 (2007), the court affirmed an unpublished Appellate Division opinion which affirmed a jury verdict awarding substantial compensatory and punitive damages and attorneys' fees against former employees and their new employer, a competitor. The employees had taken a confidential customer and sales list and installed the data on the competitor's computer system. The trial court entered partial summary judgment for liability under CROA against the former employees. The new employer/competitor was also found liable under CROA by way of a respondeat superior theory. The plaintiff employer introduced testimony by a computer expert and a forensic accountant concerning the lost profits caused by the misappropriation. The Appellate Division had upheld the damage award as sufficiently supported by expert testimony.

Honecker is a member of the litigation and alternate dispute resolution, workouts and restructurings, and insurance practice groups and is special counsel to Windels Marx Lane & Mittendorf in New Brunswick.

Fairway Dodge also sheds light on the outer limits of liability under CROA. The Supreme Court upheld the Appellate Division's conclusion that the individual owner and the manager of the competitor could not be held personally liable under the CROA because there was no evidence they personally took the data or had personal knowledge of the taking. This mens rea requirement has been applied in other cases to deny liability. See *Trading Partners Collaboration, LLC v. Kantor*, 2009 WL 12653130 (D.N.J., June 9, 2009) (insufficient evidence that defendant knowingly took data). The courts have also enforced CROA's requirement that a plaintiff must prove some damage flowing from the unauthorized access or taking to obtain a monetary award. N.J.S.A. 2A:38A-3; see also *P.C. Yonkers, Inc. v. Celebrations The Party and Seasonal Superstore, LLC*, 428 F. 3d 504, 510 (D.N.J. 2005); *Forman Industries, Inc. v. Robert Blake-Ward*, et al., Docket No. A-5581-06 (App. Div., Decided May 7, 2008).

An analogous federal statute, the Computer Fraud and Abuse Act ("CFAA") generally prohibits unauthorized accessing of a computer. The CFAA is a criminal statute that contains a civil enforcement provision, the primary focus of which concerns outside attackers, i.e., traditional hacking. See, e.g., *America Online Inc., v. Over the Air Equipment, Inc.,* 1997 WL 1071300.

Given the paucity of published opinions, a complete picture of the limits of liability under CROA remains unclear. Under a plain reading of the statute, however, CROA can be applied to a broad range of circumstances. For example, employees who impermissibly and recklessly infect their employer's computer system with viruses by accessing inappropriate and prohibited websites could be liable to the employer for damages. The specter of personal liability might lead the offending employee to agree to separation terms more favorable to the employer.

CROA's express injunctive right, backed up by CROA's broad range of monetary remedies, can be a powerful weapon, especially in emergent situations and even before serious money damages are suffered. For example, any competitor who ends up with company data on its system will have powerful incentive to quickly remove and delete such data. Access to the competitor's computer system, at least for the purpose of investigating the scope of the misappropriated data, should also be achievable.

Employers and companies should also take prudent steps to protect company data. Policies and procedures should be implemented to proscribe unacceptable use of firm data and other offensive behavior, as well as expressly spell out the company's right to protect its data. These rules should be broadly circulated, frequently, and set forth in the company's employee manual. The New Jersey Supreme Court recently affirmed employers' rights "to adopt lawful policies relating to computer use to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies." In addition, and because damaging experiences in this area frequently involve contract sales personnel, employment contracts should expressly prohibit forwarding of company data to separate systems.

In sum, employers and companies should be mindful of the potential application of CROA in disputes with employees, former employees and competitors. Creative investigative, pleading, negotiation and discovery strategies, as well as sound management of information technology, should include due consideration of the rights and remedies available under CROA.■