

EMPLOYMENT & IMMIGRATION LAW

Navigating the Minefield of Modern Employee Theft Claims

By Jeffrey M. Daitz and
Kevin J. O'Connor

With the proliferation of technology in the modern workplace, employee theft of confidential, proprietary and trade secret computer data is becoming commonplace. Remedies for aggrieved employers are available under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq. (CFAA), and its state law counterpart, the New Jersey Computer Related Offenses Act, N.J.S.A. § 2A:38A-3 et. seq. (NJCROA). But beware — a minefield awaits the attorney who sues on behalf of an employer without understanding the limitations of the CFAA.

Legislative Background

The CFAA, a federal act, provides a private right of action to those who have suffered “losses” due to violations of the act. Section 1030(a)(2)(c) imposes liability upon any person who intentionally accesses a computer without authorization

Daitz is managing partner of the labor relations and employment department at Peckar & Abramson, PC, in River Edge. O'Connor, also a partner at the firm, specializes in employment litigation.

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. Boilerplate allegations that an employee pilfered data by e-mailing confidential customer lists and other proprietary information to himself will not withstand close scrutiny at the injunction stage. See, e.g., *Trading Partners Collaboration, LLC v. Kantor*, 2009 WL 1653130 (D.N.J. June 9, 2009); *Joseph Oat Holdings, Inc. v. RCM Digesters, Inc.*, 2010 WL 5065037 (C.A.3, N.J. Dec. 13, 2010).

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, at the appellate level in *Fairway Dodge*, the court stated that 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).

Conflicting Authorities on the Scope of the CFAA

It is crucial to evaluate all aspects of the employee’s wrongful actions in drafting the complaint under both acts, and to have a thorough understanding of the relevant case law in selecting an appropriate forum for filing the complaint where there are options (as is often the case). The area that has generated the most uncertainty is whether, under the CFAA, an employee’s act of merely misappropriating data (as opposed to the traditional “hacking”) can qualify for damages where the employee “exceeded authorized access” by misappropriating data.

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 “cop-

ied” documents, as opposed to deleting or altering them.

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. Depending upon where you sue, you could get a different result entirely. Certain courts, such as the Fifth and Seventh Circuits, have applied agency law principles and have held that an employee is never authorized to access an employer’s computer in a manner inconsistent with the duty of loyalty to the employer. Applying such a rule, the moment the employee uses the computer to misappropriate proprietary information, he can be liable under the CFAA regardless of the fact that the employee had been granted such access as part of his or her duties. *United States v. John*, 597 F.3d 263, 271 (5th Cir. 2010); *International Airport Centers, LLC v. Citrin*, 440 F.3d 418, 419 (7th Cir. 2006).

In *Citrin*, where an employee erased data from company computers to cover his tracks in having formed his own business on company time and having copied data, the court held that an employee’s “authorization” for purposes of the CFAA ended the moment he violated his duty of loyalty to his employer. *Citrin*, 440 F.3d at 419. The Fifth Circuit has similarly held that an employee will violate the CFAA when he or she crosses the line and misappropriates data. *John*, 597 F.3d at 271.

Other courts have taken a stricter approach and — using a strict interpretation of the CFAA’s express language, looking to its legislative history, and applying the rule of lenity in interpreting statutes with criminal applications — have held that an employee granted access to a com-

puter cannot be held liable under the CFAA using agency principles, when he merely misappropriates data for competitive purposes. *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009).

Federal district courts within the Third Circuit have adopted this latter view, although the Third Circuit has yet to squarely address the issue. See *Bro-Tech Corp. v. Thermax, Inc.*, 651 F. Supp.2d 378, 407 (E.D. Pa. 2009); *Integrated Waste Solutions, Inc. v. Goverdhanam*, 2010 WL 4910176 (E.D. Pa. Nov. 30, 2010). Similarly, courts in the Second Circuit have held that the CFAA is to be narrowly construed and was never intended to prohibit employee misappropriation of data. *Jet One Group, Inc. v. Halcyon Jet Holdings, Inc.*, 2009 WL 2524864, at *5, 6 (E.D.N.Y. Aug. 14, 2009). The case of *U.S. v. Aleynikov*, 737 F.Supp.2d 173 (S.D.N.Y. 2010), provides an extensive analysis of the split between the Circuits in applying the CFAA.

Such cases have the effect of taking outside the statute any case where an employee merely exceeded company access in misappropriating data that he or she was otherwise authorized to work with in the course of his normal duties.

The Damage and Loss Requirements

Aside from this split of authority on the scope of the CFAA, there are many other pitfalls in litigating under the CFAA, particularly in the area of establishing “loss” or “damages.” A common tactical error is the litigant who pleads the existence of an investigation undertaken by a forensic computer expert in order to establish the \$5,000 “loss” requirement, but then finds itself in the position of having to immediately furnish the work product

of someone it regarded as an “expert” in discovery at risk of dismissal, often before that expert has undertaken a sufficient investigation. Having identified the work of the computer consultant as an “expert,” the employer will have difficulty establishing that the costs and fees billed by the expert count toward the minimal jurisdictional, statutory loss required under the CFAA. See, e.g., *B.U.S.A. Corp. v. Ecogloves, Inc.*, 2009 WL 3076042, at *7 (S.D.N.Y. Sept. 28, 2009); see also *Global Policy Partners, LLC v. Yessin*, 686 F.Supp.2d 642, 652 (E.D. Va. 2010).

Even where a litigant can show the \$5,000 jurisdictional loss required under the CFAA, a separate issue is damages. The CFAA has narrowly defined the term, severely limiting the scope of damages. The term *damage* is defined as “any impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8). The Second Circuit has ruled that the term *damages* was never intended to include lost profits when an employee steals confidential data and wrongfully competes with such data. See, e.g., *Nexans Wire S.A. v. Sark-USA, Inc.*, 2006 WL 328292, at *6 (C.A.2 (N.Y.) Feb. 13, 2006); *Jet One*, 2009 WL 2524864, at *6-7.

These and other pitfalls under the CFAA and NJCROA require that an employer’s counsel undertake a thorough review of the case law and statutes, engage the services of a qualified forensic computer expert before bringing suit, and be prepared to share the work product of that expert with the defendant in initial discovery. Careful attention to the pleadings is required, and the employer must be prepared to make full disclosure at an early stage of both the minimal jurisdictional loss and the proofs needed to establish the claims under the acts. ■

