Bloomberg Law Reports® Technology Law

The Computer Fraud and Abuse Act: A Weapon Against Employees Who Steal Trade Secrets

Contributed by Holly R. Rogers and Katharine V. Hartman, Dilworth Paxson LLP

The Computer Fraud and Abuse Act (the "Act") is a criminal statute that provides a civil cause of action for anyone whose computer system or network has been damaged or accessed without authorization, provided certain requirements are met. Although traditionally thought of as a form of relief for those who fall victim to computer "hackers," the Act has seen increased use in the employer-employee context.

Specifically, employers are increasingly using this cause of action to go after former employees who steal trade secrets from their company-issued computers.[1] As the Third Circuit Court of Appeals has acknowledged: "the scope of [the Act's] reach has been expanded over the last two decades. Employers are increasingly taking advantage of [the Act's] civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system."[2] Notably, the body of case law recognizing that the Act extends to wrongful actions more typically the subject of trade secret theft litigation seems only to be growing.

Since most businesses keep their proprietary and confidential information on computers, the Act can frequently be invoked to address the theft of this information. The typical fact pattern in an employer-employee case involves a departing or disgruntled employee copying trade secrets or other confidential business information from the company's computer systems. This theft might be done by using a portable USB device, by emailing the information to a personal email account, or by logging into a password protected computer system. The employee then will frequently use computer wiping software in an attempt to cover up their theft. The Act provides a mechanism for redressing the harm that employers suffer when their employees take these kinds of actions against them.

The Advantages of Bringing a Claim Under the Act

Employers stand to benefit from bringing a claim under the Act for several reasons.

The Act is first and foremost a criminal statute. Bringing a claim against an ex-employee under a criminal statute emphasizes the serious nature of the employee's wrongful actions. You will therefore rightfully get the attention of your former employee by alleging violations of the criminal Act. Taking aggressive action under a criminal statute will also serve as a warning to any of your current employees who may be contemplating stealing your information or causing mischief by hacking into your computer system or otherwise destroying your valuable information.

The Act also allows you to assert a claim that looks like trade secret theft without actually having to

prove that the employee stole a "trade secret." Not all confidential information rises to the level of a legally protectable trade secret, but is nonetheless valuable to its owner. Claims under the Act focus on how the employee wrongfully accessed the information and not on proving that the content of the accessed information rises to the level of a trade secret.

Bringing a claim under the Act is also attractive because of the legal remedies available to a prevailing plaintiff under the Act. The statute specifically creates a private cause of action with injunctive relief as an appropriate remedy.[3] Courts have concluded that the type of injunctive relief available to a plaintiff in a cause of action brought pursuant to the Act includes prohibiting operation of a competing business, prohibiting use of unlawfully obtained information, and ordering the return of such information.[4] The availability of injunctive relief under the Act may be attractive where you seek to quickly enjoin a former employee from using stolen confidential information without having to go through the trouble and difficulties of showing the likelihood that it was a trade secret that was stolen. Additionally, if your employee is not prevented from competing with you through a restrictive covenant, the Act provides a tool for ensuring that the employee cannot use information that he wrongfully obtained from you to compete with you.

Finally, the Act may enable you to file your complaint in federal court. Because the Act provides for federal question subject matter jurisdiction, adding a cause of action for a violation of the Act automatically gets you into federal court. The federal court where you file your complaint will then have supplemental jurisdiction over any common law claims that you bring under state law.

Unresolved Legal Issues Under the Act

The case law interpreting the Act in the employer-employee context is relatively dynamic at this time. Accordingly, it is critical that you know the current case law interpreting the Act in your jurisdiction before you draft and file your complaint.

The principle unresolved legal issues impacting employer-employee claims under the Act include what actions constitute unauthorized access under the Act and what kinds of damages count towards the Act's $5,000 jurisdictional threshold.

The remainder of this article will summarize how some of the different Circuit Courts that have addressed these issues have resolved them and will provide related helpful hints for drafting a complaint sufficient to survive a Rule 12(b)(6) challenge.

What Actions Constitute Unauthorized Access or Exceeding Authorized Access Under the Act?

The Act provides a civil cause of action against anyone, inter alia, who, inter alia, has been injured by damage caused to or wrongful access of a protected computer without authorization or in excess of their authorization.

Although the Act does not define "authorization" or "without authorization," it has been held that an employee does not have authority to access his work computer once he violates his duty of loyalty to his employer.[5]

For example, in *Citrin*,[6] an employee decided to quit and go into business for himself.[7] Before returning his company-issued laptop, the employee deleted all the data in it, including data he had collected and which would have revealed improper conduct.[8] Specifically, the employee loaded into the laptop a computer wiping program, which wrote over deleted files to prevent their recovery.[9]

The *Citrin* Court held that the employee was "without authorization" to delete his employer's computer files and run computer wiping software to cover his tracks.[10] Notably, the court said that the employee's "authorization to access the laptop terminated when, having already engaged in mis-

conduct and decided to quit . . . he resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee."[11] Because the employee's only authority to access the laptop was based on the agency relationship with his employer, the authority to access the laptop ended as soon as the employee breached his duty of loyalty by acting in his own interests and in spite of his employer's.[12]

It has also been held that an employee "exceeds authorization" if the employer has policies that prohibit accessing information for non-business reasons.[13] The Act itself defines the term "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[14] In *Rodriguez*, the Court of Appeals for the Eleventh Circuit applied this definition to an employee who accessed information on his employer's database for non-business reasons.[15] Because such access was in violation of company policy, the employee was found to have exceeded authorized access and thus to have violated the Act.[16]

Recently, the Court of Appeals for the Ninth Circuit in *United States v. Nosal*[17] adopted the approach taken in *Rodriguez*, finding that the employee "exceeds authorization" when there are use restrictions in place that the employee has violated, stating "as long as the employee has knowledge of the employer's limitations on that authorization, the employee 'exceeds authorized access' when the employee violates those limitations. It is as simple as that."

What Qualifies As "Loss" Sufficient to Meet the $5,000 Jurisdictional Threshold?

Assuming that you are able to allege that the employee violated the Act, you must still show that the type of violation committed falls within the civil remedy provision of the Act.[18] The civil remedy provision of the Act provides in pertinent part: "A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)."[19]

In most cases, the subsection that the employee's conduct will fall within involves the factor set forth in subclause (I), namely, "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value."[20] "Loss" is defined under the Act as: "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[21]

For example, the cost to hire a computer forensic consultant to conduct a damage assessment, including examination of what files or data have been deleted or overwritten, has been included in the $5,000 threshold calculation.[22] This is true even if no physical damage is actually found.[23] As the Court of Appeals for the First Circuit recognized, it would flout Congressional intent to require that physical damage be found during such damage assessments.[24] That court explained: "As we move into an increasingly electronic world, the instances of physical damage will likely be fewer while the value to the victim of what has been stolen and the victim's costs in shoring up its security features undoubtedly will loom ever-larger."[25]

Hints for Drafting Your Complaint

If you decide to bring a claim under the Act, you must first educate yourself on the case law interpreting the Act in your jurisdiction so that you know exactly what allegations are needed to state a bullet-proof claim under the Act. Regardless of your jurisdiction, however, including the following allegations in your complaint will likely help prevent you

from being on the losing end of a **Rule 12(b)(6)** challenge:

- the employee accessed a protected computer used in interstate commerce
- the employee was without authorization to access the computer and/or exceeded authorization
- the employee's actions violated the duty of loyalty to the employer
- the employee violated the employer's policies by accessing the information
- the employee's actions caused loss in excess of $5,000 to your computer files, programs, systems, information or other data
- the employee's actions caused loss in excess of $5,000 due to an interruption in service
- the employer responded to the employee's offenses by hiring an external computer forensic consultant to conduct a damage assessment, including but not limited to assessment of permanently deleted, altered or erased files, programs, usage history, and other data, along with computer wiping software used on the employer's computers (if any)
- the computer forensic consultant also investigated, analyzed and attempted to recover destroyed data and information from the employer's computers
- the employee caused an impairment to the integrity or availability of data, a program, a system, or information

Keep in mind that you need to look at the specific facts of your case to determine what, if any, of the Act's subsections are applicable and which of the above suggestions are appropriate in your case. Depending on your particular situation, this list may need to be expanded. The important take away is that the case law interpreting the Act continues to provide an opportunity for you to take your employees to task for stealing your trade secrets.

Holly R. Rogers (hrogers@dilworthlaw.com) (A.B., Harvard University; J.D., Duke University) and Katharine V. Hartman (khartman@dilworthlaw.com) (B.A., University of Florida; J.D., Duke University) practice labor and employment law at Dilworth Paxson LLP in Philadelphia, Pennsylvania.

---

1 The Act only applies to a "protected computer," defined in the Act as a computer "which is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). If your impacted computers are connected to the internet and are used for conducting business throughout the United States and/or across the globe, you should be able to successfully claim that your computer is protected under the Act.

2 *P.C. Yonkers, Inc. v. Celebrations! The Party & Seasonal Superstore, LLC,* 428 F.3d 504, 510 (3d Cir. 2005) (internal quotations and alterations omitted).

3 18 U.S.C. § 1030(g); *see also P.C. Yonkers*, 428 F.3d at 508 (confirming the availability of injunctive relief under the Act).

4 *See, e.g*., *P.C. Yonkers*, 428 F.3d at 507, 511 (concluding that the type of injunctive relief available to a plaintiff in a cause of action under the Act includes prohibiting operation of a competing business, prohibiting use of unlawfully obtained information, and ordering the return of such information); *EF Cultural Travel BV EF v. Explorica,* 274 F.3d 577, 585 (1st Cir. 2001) (affirming grant of preliminary injunction under the Act); *Southeastern Mechanical Services, Inc. v. Brody*, No. 08-CV-01151, 2008 BL 232599 (M.D. Fl. Oct. 15, 2008) (recognizing that irreparable harm in case brought pursuant to the Act includes harm to existing customer relationships, reputation in the industry, and goodwill); *Yournetdating, LLC v. Mitchell*, 88 F. Supp. 2d 870 (N.D. Ill. 2000) (granting TRO based on irreparable harm in form of damage to goodwill).

5 *See Intl. Airport Centers, LLC v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006); *see generally* 18 U.S.C. § 1030(e) (Act's definition section); *see also P.C. Yonkers,* 428 F.3d at 510 (acknowledging that, included within the scope of the Act are claims by employers against former employees and their new companies who seek a competi-

tive edge through wrongful use of information from the former employer's computer system).

6 440 F.3d 418.

7 *Id.* at 419.

8 *Id.*

9 *Id.*

10 *See Citrin*, 440 F.3d at 420.

11 *Id.*

12 *Id.*

13 *See United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010).

14 18 U.S.C. § 1030(e)(6).

15 628 F.3d at 1263.

16 *Id.*

17 No. 10-10038, 2011 BL 114050 (9th Cir. Apr. 28, 2011).

18 *See* 18 U.S.C. § 1030(g).

19 *Id.*

20 18 U.S.C. § 1030(c)(4)(A)(i)(I).

21 18 U.S.C. § 1030(e)(11).

22 *See, e.g., EF Cultural Travel,* 274 F.3d at 585 (finding that "loss" under the Act for purposes of the $5,000 threshold includes sums spent to assess the extent of physical damage caused by intrusion onto a company's website, even if it is found that no physical damage was actually done); *P.C. Yonkers, Inc. v. Celebrations! The Party & Seasonal Superstore, LLC*, No. 04-4554 (JAG), 2007 BL 229567, * 8-10 (D.N.J. March 5, 2007) (finding that "loss" under the Act for purposes of the $5,000 threshold includes sums spent "responding to" and "investigating defendants' actions" as well as "taking remedial steps to prevent defendant's further actions")*; Kalow & Springnut, LLP v. Commence Corp*., No. 07-3442, 2009 BL 1226 at *5-6 (D.N.J. Jan. 6, 2009) (finding threshold amount includes wages or fees paid to computer consultants); *B&B Microscopes v. Armogida*, 532 F. Supp. 2d 744, 753, 758-59 (W.D. Pa. 2007) (finding threshold amount satisfied by cost of forensic damage assessment where employee selectively deleted and overwrote thousands of files from his company laptop); *Hudson Global Resources Holdings, Inc. v. Hill*, No. 07-CV-00132, 2007 BL 190879 at *3-5 (W.D. Pa. March 2, 2007) (finding that "loss" under the Act for purposes of the $5,000 threshold includes sums spent on consultant retained to investigate and analyze extent to which employee misappropriated information from employer's computer network).

23 *See EF Cultural Travel,* 274 F.3d at 585.

24 *Id.*

25 *Id.*