

I. Computer Fraud and Abuse Act

The federal Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, provides for the punishment of anyone who, among other acts,

Intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer if the conduct involved an interstate or foreign communication, 1030(a)(2)(C);

Knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period, 1030(a)(4); or

Intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and by conduct described in clause (iii) of subparagraph (A), caused loss to 1 or more persons during any 1-year period aggregating at least \$5,000 in value, 1030(a)(5)(A)(iii) and (a)(5)(B)(i).

Subsection (g) provides for a civil cause of action against the violator for compensatory damages and injunctive relief, as long as the conduct involves an action under (a)(5)(B)(i). Damages for a violation involving conduct of subsection (a)(5)(B)(i) are limited to economic damages.

Congress amended the CFAA to expand the CFAA’s scope to include civil claims challenging the unauthorized removal of information or programs from a company’s computer database. Pacific Aerospace & Electronics, Inc. v. Taylor, 295 F.Supp.2d 1188, 1196 (E.D. Wash. 2003). Thus, employers “are increasingly taking advantage of the CFAA’s civil remedies to sue former employees and their new companies who seeks a competitive edge through wrongful use of information from the former employer’s computer system.” Id. Most importantly for our purposes, while a violation of the CFAA may also implicate rights under various intellectual property statutes (e.g, copyright or more commonly trade secrets), the crux of an offense under the CFAA is the abuse of a computer to obtain information. Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F.Supp.2d 1121, 1128-29 (W.D. Wash. 2000). This means that anyone who wrongfully takes information, whether a trade secret or not, is in violation of the CFAA.

In Shurgard, the plaintiff former employer sued its former employees and the defendant competitor for whom the employees went to work. The defendant had offered a job to one of the employees, and, “while still employed by the plaintiff, but acting as an agent for the defendant, [the employee] sent e-mails to the defendant containing various trade secrets and proprietary information belonging to the plaintiff.” The defendant subsequently hired the employee. 119 F.Supp.2d at 1123.

The district court concluded that the plaintiff had stated a claim that the employee, and thus the defendant, had violated subsection (a)(2)(c) the CFAA because the employee had accessed plaintiff's information without authorization. Relying on the Restatement (Second) of Agency, which states that "the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal," the district court concluded that the employees' authority ended when they became agents for the defendant, and this the employees were "without authorization" when they obtained and sent the proprietary information to the defendant via e-mail. Id. at 1125.

Similarly, the district court held that the plaintiff had stated a claim against the employees and defendant under subsection (a)(4) because the word "fraud" in the context of the CFAA means simply wrongdoing on the part of the violator, and not proof of the common law elements of fraud. Id. at 1125-26. Finally, the plaintiff stated a claim under subsection (a)(5)(C) because the district court interpreted the word "damage" to include the employee's actions in collecting and disseminating confidential information, thereby impairing the "integrity" of the plaintiff's information. Id. at 1126-27.

The type of damage or loss that allows for recovery under the CFAA has also been broadly interpreted in EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001). The First District Appellate Court affirmed the district court's reasoning that a general understanding of "loss" would "fairly encompass a loss of business, goodwill, and the cost of diagnostic measures that EF took after it learned of Explorica's access to its website." Id. at 584. The court concluded by stating that "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." Id. at 585.

In Taylor, the district court, relying on Shurgaurd, reached the same conclusion regarding the defendants' taking of information from their former employer's computer. 295 F.Supp.2d at 1195-96. Most relevant for our case, although not involving the CFAA, the district court granted the former employer a preliminary injunction for trade secret misappropriation, based in part upon defendants' compilation of "a list of prospective customers ... from their memories and business card file Taylor retained when he left." Id. at 1193, 1200.

Finally, in Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A., the district court found the defendants liable for accessing the plaintiff's customer database without authorization, and awarded the plaintiff \$2,090,000, the value of the customer information that the defendant wrongfully obtained, plus \$28,000 in expenses the plaintiff incurred in investigating and responding to the various violations, all of which occurred within a one-year period. 267 F.Supp.2d 1268, 1323-24 (S.D. Fla. 2003). Additionally, based upon the defendant's intentional deletion of information from one of its computers after the court had ordered the computer produced for inspection, the district court drew an adverse inference to defendant that the deleted information constituted confidential customer and financial data of the plaintiff. Id. at 1322, n.1.