HINSHAW

How Employers Can Use the Computer Fraud and Abuse Act to Their Advantage

Labor and Employment Newsletter - May 2018

Hinshaw Newsletter | 6 min read
May 2, 2018

Every employer has to contend with employee turnover, including key personnel leaving for a competitor. The loss or compromise of confidential data is a significant risk in such a scenario. One way for an employer to protect itself is by resorting to the Computer Fraud and Abuse Act (CFAA), a civil remedy that allows a private party to seek compensation for losses caused by the unauthorized access to data on a protected computer by a current or former employee.

There is a split in the federal circuits regarding the interpretation of "unauthorized access" under the CFAA. We will explore this split, and also provide an analytical framework for employers to use when assessing the prospects of pursuing a CFAA claim.

Statutory Background

The CFAA is a statutory provision that was part of the Comprehensive Crime Control Act of 1984 passed by Congress. Pub. L. 98-473, S. 1762, 98 Stat. 1976, enacted October 12, 1984). It contains a civil remedy provision whereby a private party may seek compensatory damages and equitable relief upon satisfying elements that require pleading proof of recoverable damage or loss that occurred within one year of the date of the complained of loss or discovery of the damage. 18 U.S.C. 1030(g). *Id.* To plead a claim under the CFAA, one must sufficiently allege that a defendant: (1) intentionally accessed a computer; (2) lacked authority to access the computer or exceeded granted authority to access the computer; (3) obtained data from the computer; and (4) caused a loss of $5,000 or more during a one year span. *Clarity Services, Inc. v. Barney,* 698 F.Supp.2d 1309, 1313 (M.D. Fla. 2010); *Continental Group, Inc. v. K.W. Property Management, L.L.C.,* 622 F.Supp.2d 1357, 1369-71 (S.D. Fla. 2009); *Ill. Corp. v. A-1 Tool Corp.,* 714 F.Supp.2d 863, 876 (N.D. Ill. 2010). Restated, employers must satisfy the cited elements of the CFAA when pleading their story about how a defendant improperly accessed a protected computer with the intent to defraud. *Id.*

© 2025 Hinshaw & Culbertson LLP

The CFAA covers a "protected computer," and speaking beyond the servers of the United States government or a financial institution, the CFAA defines a "protected computer" as meaning a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States [.]" 18 U.S.C. 1030(e)(2)(B). Most employers pursuing a CFAA claim against a current or former employee—and against the employee's new employer or business venture—will find coverage for their computers under the general provision on protected computers.

Split in the Circuits Regarding "Access without Authorization"

Litigation involving the CFAA often revolves around the absence of any definitions in the CFAA of the terms "access" or "without authorization." The CFAA defines "exceeds authorized access," as meaning "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." 18 U.S.C. 1030(e)(6). The lack of a statutory definition of what qualifies as "access," or accessing a computer "without authorization," however, has created a split between the Circuits of the U.S. Court of Appeals over what actions by an employee qualify as exceeding authorized access under the CFAA.

The First, Fifth, Seventh, and Eleventh Circuits of the U.S. Court of Appeals broadly read the CFAA as covering employees who misuse data obtained from an employer-provided computer—even when the employee was authorized to obtain data from the employer's computer. Some of these courts even use common-law agency and duty of loyalty principles when interpreting the CFAA. As a general rule, these courts focus on the employer's computer use policies and the intended use of the data by the employee as significant factors when determining whether the CFAA covers the employee's complained of access and use of data from the employer's computers. See *United States v. Rodriguez,* 628 F.3d 1258, 1263 (11th Cir. 2010), *cert. denied,* 563 U.S. 966 (2011) *United States v. John,* 597 F.3d 263, 272 (5th Cir. 2010), *cert. denied,* 568 U.S. 1163 (2013; *Int'l Airport Ctrs., L.L.C. v. Citrin,* 440 F.3d 418, 420-21 (7th Cir. 2006); and *EF Cultural Travel BV v. Explorica, Inc.,* 274 F.3d 577, 581-84 (1st Cir. 2001).

The Fourth and Ninth Circuits—and arguably the Second Circuit—however, narrowly interpret the CFAA as focused on whether the employee's access to an employer's computer was authorized and disregard or downplay the misuse analysis. See *United States v. Valle,* 807 F.3d 508, 526-28 (2nd Cir. 2015)=; *WEC Carolina Energy Solutions LLC v. Miller,* 687 F.3d 199, 203-07 (4th Cir. 2012); and *LVRC Holdings L.L.C. v. Brekka,* 581 F.3d 1127, 1135 (9th Cir. 2009).

The Supreme Court had an opportunity to resolve the ongoing dispute over how to interpret the CFAA with respect to authorized access to employer computers at the workplace two years ago. The Court, however, did not provide any insights or practical construction of the CFAA statutory term "without authorization." *Musacchio v. United States,* 136 S.Ct. 709 (2016).

Analytical Checklist for Evaluating a Potential CFAA Claim

In light of the existing disagreement between the Circuits of the U.S. Court of Appeals, recent case law suggests what an employer may look for as focal points to drive its analysis of a potential CFAA claim.

1. Does the claim include a factual scenario that occurred in or impacted a jurisdiction that currently uses a broad interpretation of what employee conduct qualifies as exceeding authorized access under the CFAA? *Hamilton Grp. Funding, Inc. v. Basel,* No. 16-61145-CIV, 2018 BL 131830, **11-13 (S.D. Fla. Apr. 12, 2018).
2. If the judicial forum for your case restricts claims against employees with authorized access to an employer's computers, do the facts support pleading an indirect-access theory and naming non-employee individuals, competitors, or contractors as co-defendants along with the former employee? Did someone act in concert with the employee to access information beyond what the employee was authorized to access? *Teva Pharm. USA, Inc. v. Sandhu,* No. 17-3031, 2018 US Dist LEXIS, 14470, 2018 BL 30491,*6 (E.D. Pa. Jan. 30, 2018); and *Space Sys./Loral, LLC v. Orbital ATK, Inc.,* No. 4:17-cv-00025, 2018 WL 701280, 2018 BL 36146,*4 (E.D. Va. Feb. 2, 2018).
3. Did the employee commit acts that damaged the employer's protected computer after the employee resigned or was terminated? Such actions may qualify as access lacking any authorization so as to avoid the quandary over whether an employee exceeded authorized access under the CFAA. This line of case law highlights the need to implement clear and consistent procedures for ending and revoking an employee's access to an employer's computers at the end of the employment relationship. *UCAR Technology (USA) Inc. v. Yan Li,* No. 5: 17-cv-01704, 2017 BL 450429,**5-6 (N.D. Cal. Dec. 15, 2017); and *LVRC Holdings LLC v. Brekka,* 581 F.3d 1127, 1136 (9th Cir. 2009).
4. In addition to gathering evidence that satisfies the $5000 damage requirement of the CFAA—can the employer identify egregious digital misconduct that is easily understood as offensive so as to persuade a court to find CFAA coverage? Such persuasive damage may include: an employee who stops a computer system from providing backups, deletes files outside the normal workplace procedures, falsifies contact information in a computer notification system, or who initiates a process that prevents users from remotely accessing the employer's network. Such evidence highlights the impairment to the employer's computer networks and may increase the likelihood of a court interpreting the CFAA in the employer's favor. *United States v. Thomas,* 877 F.3d 591, 598-99 (5th Cir. 2017).

Conclusion

Many employers are understandably hesitant about using the CFAA as a litigation tool. Their outside counsel and legal news articles often highlight the discord that exists over a central issue posed by the CFAA: what conduct by employees qualifies as exceeding their authorized access to an employer's protected computer system? However, in light of the ever increasing threats posed by internal violations of employers' cyber security policies and protocols, employers should prioritize finding evidence that supports the core elements of a viable claim under the CFAA. As we have seen, there are some consistent lines within the CFAA case law that can support a viable CFAA claim regardless of jurisdiction. Taking concrete steps such as drafting helpful computer use policies, implementing consistent computer access revocation procedures, and compiling key relevant evidence, can increase the likelihood of a pursuing a CFAA claim and developing a winning litigation strategy.

Employment Law Observer Blog

Since the last edition of the Labor & Employment Newsletter, our employment blog has published several posts, including:

- *NFL's Termination of Security Personnel Prompts Allegations of Age Discrimination*
- *Use of Salary History Taboo? Ninth Circuit Weighs In*
- *California Supreme Court to Provide Guidance on Meal and Rest Breaks*
- *Temporary Schedule Changes Now Mandatory for New York City Employers*

This newsletter has been prepared by Hinshaw & Culbertson LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship.

Related People

Ambrose V. McCall

Partner

309-674-1025

Related Capabilities

Labor & Employment