Cybersecurity Threats from Within: How the Computer Fraud and Abuse Act Can Be Used to Combat Employee Theft of Trade Secrets

Given the relative ease in which employees can access, copy, store, and transport confidential and proprietary company data, cyber-security threats from within an organization are of mounting concern. While preemption is first and foremost the preferred course, companies that have been victimized by the theft or destruction of their data have various means of legal redress, whether the perpetrator is an employee or not. This post discusses one possible avenue of relief for employers to consider in the event they find themselves the target of employee digital theft—the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA" or the "Act").

Originally enacted in 1984 to punish remote computer hackers, the CFAA has been increasingly used by employers as a legal remedy against employee theft, destruction, or misuse of confidential and proprietary data stored on company computers. The CFAA imposes both civil and criminal liability for accessing a computer "without authorization" or "exceeding authorized access" and then taking various unlawful actions, such as stealing or deleting information stored on a computer.

Unlike state trade secrets law—which generally requires proof that the data is in fact secret and that reasonable measures were taken to maintain its secrecy—the CFAA only requires that the employee accesses the company's computer "without authorization" or that the employee exceeded authorized access, regardless of whether the data at issue technically qualifies as a trade secret.

Unfortunately, neither the term "without authorization" nor the word "authorization" is defined by the CFAA. While the CFAA does define "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," 18 U.S.C. § 1030(e)(6), the exact parameters of what constitutes "authorized access" have yet to be definitively delineated.

A company can generally readily establish a CFAA violation in the case of *remote* hackers (*i.e.*, individuals who have no authorized access to a company's computer at all). The question regarding if and under what circumstances an employee—who generally has permission to use the company computer in the course of his or her job duties and may even

have "authorized" access to the proprietary material at issue—can violate the CFAA is much trickier.

For the most part, courts have adopted one of two positions when interpreting the CFAA in the case of *inside* hackers (*i.e.*, individuals whose initial access to a computer is authorized but who access unauthorized information or files). Under a *narrow interpretation*, which has been adopted by a majority of courts, any data accessed by an employee on a server for which he or she has permission to access would be with authorization, regardless of the employee's motive in accessing the data or how it is ultimately used. Under this view, access to a protected computer occurs "without authorization" only if the initial access was not allowed, and a violation for "exceeding authorized access" occurs only if the access to the computer is beyond what is initially permitted—say, for example, an employee is authorized to access only product information, but he instead accesses financial data or customer lists.

Below are examples of court opinions following the narrow interpretation—which include federal courts sitting in the Ninth Circuit (Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, Oregon, and Washington) and Fourth Circuit (Maryland, North Carolina, South Carolina, Virginia, and West Virginia):

- *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (finding *no* CFAA violation where employees of executive search firm used their log-in credentials to download source lists, names and contact information from a confidential database on employer's computer, and then transferred that information to competitor, in violation of company policy)
- *WEC Carolina Energy Solutions LLC v. Miller*, 687 F. 3d 199 (4th Cir. 2012) (finding *no* CFAA violation where employee downloaded company's confidential and proprietary information to his personal computer in violation of company policy, and used it in making a presentation for a competitor)

By contrast, under a *broad interpretation* of the CFAA, wherever an employee breaches a duty or loyalty, or a contractual obligation, or otherwise acquires an interest adverse to the employer, their authorization to access information stored on an employer's computer terminates and all subsequent access is unauthorized/exceeds the scope of authorization. Under this view, an employee would exceed the scope of his or her authorized access if data accessed from the company's server was used for any purpose prohibited by a company's computer use policy. For example, an employee may be authorized to access customer lists in order to do his job—a corporate policy

"yes"—, but not to send them to a competitor—a corporate policy "no."

The following are examples of court opinions following the broad interpretation, adopted in the Fifth (Louisiana, Mississippi, and Texas), Seventh (Illinois, Indiana, and Wisconsin), Eighth (Arkansas, Iowa, Minnesota, Missouri, Nebraska, North Dakota, and South Dakota), and Eleventh (Alabama, Florida, and Georgia) circuits:

- *U.S. v. John*, 597 F.3d 263 (5th Cir. 2010) (CFAA violation found where use of information obtained by permitted access was illegal; specifically, account manager accessed customer account information contained in Citigroup's internal computer system and shared information with half-brother to incur fraudulent charges)
- *U.S. v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (CFAA violation found where TeleService representative of Social Security Administration accessed government database containing sensitive personal information for nonbusiness reasons)
- *International Airport Centers LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006) (CFAA violation found where employee permanently deleted all data on company laptop prior to quitting his job in violation of his employment contract)

Practical Steps

In light of the split in court opinion regarding the reach of the CFAA in combating employee theft of trade secrets or other confidential and proprietary business information, the success of a CFAA cause of action may well hinge on the jurisdiction in which the suit is brought, at least until the Supreme Court weighs in on the issue. Nevertheless, employers should consider implementing the following measures, which may not only serve to bolster an employer's CFAA claim against disloyal employees—while also serving as a basis for raising breach of contract, trade secret misappropriation, and related state law claims if the federal CFAA claim is otherwise unavailing—but also minimize the potential of data theft or misuse in the first place:

- Adopt clear and conspicuous computer access and use policies prohibiting disclosure to outside parties and restricting access for nonbusiness purposes
- Draft the computer access and use policies to prohibit not only intentions (*e.g.*, "for legitimate business purposes only") but also – and more importantly – actions (*e.g.*, theft, destruction, *etc.*)

- Limit access to company information on a strict need-to-know basis, and tighten access controls on company systems and databases
- Limit an employee's access solely to those portions of the computer systems and databases which are required for the employee to perform his/her job
- Implement log-in notifications, alerting employees that information contained on the company's servers, computers, and databases is the company's data and that unauthorized use and access could lead to disciplinary action and criminal prosecution
- Limit access to computers to those assigned individual passwords, and prohibit employees from sharing their passwords with others
- Provide that an employee's authorization to access company information, including confidential information of the employer, ceases immediately upon termination, receiving an offer of employment elsewhere, or other triggering event

If you have any questions about this article, please contact:

Robert McHale, Esq.
R | McHale Law
9 West Broadway, Suite 422
Boston, MA 02127
Tel. 617.306.2183
Email: robert.mchale@rmchale.com