



Employees Who Take Proprietary Data May Violate the Federal Computer Fraud and Abuse Act

March 2009

Has your company either been the subject of a competitor's raid of your key employees or have any of your employees resigned to start a competing venture? Did you worry that they had taken your proprietary information with them and used it to unfairly compete against you? You should.



W. Michael Holm

A recent article in the *Washington Business Journal* (Feb. 23, 2009), [click here](#), reported the results of a survey of 1,000 individuals who had changed jobs during 2008. According to the survey, 59 percent of the respondents stole confidential company data in the process of leaving. That data included email lists and customer information. And, of those who purloined the data, 67 percent used the information to benefit their new employer.



James B. Kinsel

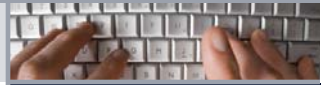
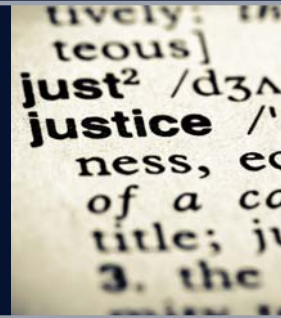
Such conduct often results in companies bringing claims against the departing employees and possibly their new employers for conversion, interference with contract or business expectancy, breach of fiduciary duty and/or business conspiracy. Another type of claim gaining traction nationwide is that the conduct violates the federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, thus creating a federal cause of action for conduct that, otherwise, would be limited to claims based on state law.

The CFAA is a criminal statute that provides a civil remedy as well. In short, among other things, the Act makes it unlawful for a person to intentionally access a protected computer without authorization or by exceeding such authorization and (1) obtain information; or (2) knowingly and with intent to defraud and in furtherance of the fraud obtain something of value, unless the only thing obtained is the use of the computer and that use is not valued at more than \$5,000 in a one-year period. The CFAA also makes it unlawful to intentionally access a protected computer without authorization and cause damage "to the integrity or availability of data, a program, a system or information." In general, a plaintiff must demonstrate damage or loss from the conduct at issue aggregating at least \$5,000 in value during a one-year period.

The Act's potential applicability to a departing employee's actions turns on whether the employee was authorized to access the computer or exceeded his authorized access when he took the proprietary information, permanently deleted it or damaged the computer. Under most circumstances, the employee was authorized to access the computer system as a condition of employment. Of course, former employees risk significant exposure under the Act if they access a former employer's computer without permission.

Courts have wrestled with how to determine whether the offending employee accessed a computer without authorization or exceeded his right of access. Under the Act "exceeds

continued



Computer Fraud and Abuse Act. © 2009 Williams Mullen.

Editorial inquiries should be directed to W. Michael Holm, 703.760.5225 and mholm@williamsmullen.com, or James B. Kinsel, 703.760.5251 and jkinsel@williamsmullen.com.

This information is provided as an educational service and is not meant to be and should not be construed as legal advice. Readers with particular needs on specific issues should retain the services of competent counsel.

www.williamsmullen.com

authorized access” means “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.” Some courts have based their analysis on a consideration of any restrictive covenant or agreement regarding the confidentiality of information that the employee signed while employed. See *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001). Others, and most notably the federal 6th Circuit Court of Appeals have used an agency theory as their measuring stick. *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (6th Cir. 2006).

Under the agency theory, the employee owes a duty of loyalty to his employer to act only on behalf of and in the interest of the employer. When the employee makes plans to leave and join a competitor or form his own firm and decides to take with him proprietary data owned by his employer, he breaches that fiduciary duty because he appropriates the data to further his own interests and not those of his employer. Accordingly, at that point in time, his authorization to access the data at issue terminates. Moreover, any attempt to access a computer and take proprietary data would also exceed the limits of the employee’s authorization, thus, violating the Act. As one court put it, “the authority of the 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.” *Citrin*, 440 F.3d at 421.

A number of courts have followed the 6th Circuit’s view and applied the agency approach to CFAA claims. Others have rejected it as being too broad in application. There are no decisions from the federal court in the District of Columbia on the point. A decision from the District Court in Maryland rejected the agency theory. *International Assoc. of Machinists and Aerospace Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479 (D. Md. 2005) Finally, the Eastern District of Virginia has considered the issue once and, while recognizing the agency approach, found that it did not fit the facts of the case before the court. *Secureinfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593 (E.D. Va. 2005). Both the Maryland and Virginia cases, however, predate *Citrin*.

One question missing from discussion in the cases addressing the agency theory is which law to apply in determining the applicable agency principles. Plainly, there are differences among the states. Which law to apply or if some federal common law would apply are issues that, for now, are unresolved. They are not insignificant, however, because either approach risks creating inconsistencies. If state agency laws apply, the CFAA might be inconsistently applied because conduct that violated one state’s agency law may be permissible conduct in another state. On the other hand, if the CFAA created new federal common law, a person could be subjected to two different tests for the same conduct: (1) a state’s common law, and (2) federal common law borrowed from whatever sources a particular judge may deem applicable.

In the future, whether the courts in the Washington, D.C. area will follow the agency approach and find rogue employees guilty of violating the CFAA when they take proprietary information with them to a new employer remains to be seen. For now, however, it is potentially a potent weapon against the misappropriation of proprietary data.

For more information on this topic, please contact W. Michael Holm, mholm@williamsmullen.com, 703.760.5225; or James B. Kinsel, jkinsel@williamsmullen.com, 703.760.5251. Mr. Holm and Mr. Kinsel are also the authors of the Unfair Business Practices blog (<http://unfairbusinesspractices.blogspot.com/>).