Preserving a CFAA Claim When Employees Misappropriate Data

05.26.2011

Louis B. Meyer III
Elizabeth H. Johnson

The Computer Fraud and Abuse Act (the "CFAA") imposes criminal penalties when a "protected computer" is accessed "without authorization." Because the CFAA applies to any computer used in foreign or interstate commerce, computer systems used by most businesses are protected by the law. As a result, the CFAA's ban on unauthorized access is frequently cited in cases against hackers and other unauthorized third parties that intrude on a company's information systems. The statute has other purposes, however, such as prohibiting authorized users from "exceeding authorized access." Since the CFAA provides for civil enforcement of these prohibitions, the statute also can be useful to employers that want to recover against employees who have abused their access rights to misappropriate company information. Historically, courts have been reluctant to advance CFAA claims by employers, expressing concern at the prospect of holding employees civilly or criminally liable for their use of computer systems. In order to preserve a CFAA claim, employers must understand and appreciate the nuances of courts' interpretations of this statute and apply that knowledge to their acceptable use policies and employment agreements. In this Alert, we review some recent cases bearing on this issue, and present a list of practical tips to help preserve a CFAA claim.

A recent decision by the U.S. Court of Appeals for the Ninth Circuit, *United States v. Nosal*, provides helpful reasoning on the supportability of CFAA claims. In *Nosal*, the court held that a company's former employees could be held criminally liable under the CFAA for exceeding authorized access to the company's computer system when he engaged some of the company's current employees to help him set up a rival business. The employees he recruited

downloaded and sent to him the company's valuable proprietary information from its password-protected database prior to leaving their jobs. The employees had signed employment agreements with the company prohibiting them from disclosing such information to third parties or using it for any purposes other than legitimate business purposes. In addition, the company had a written computer use policy that prohibited employees from accessing its computer system and disclosing information in the system to outside parties or making any use of the information other than for legitimate business purposes. This policy was made clear to employees when they were hired and was reiterated each time they logged on to the company's computer system.

The court in *Nosal* held that an employee "exceeds authorized access" under the CFAA when he or she violates the company's computer access and use restrictions. Because the company had prohibited its employees, by contract and in a written policy, from accessing its computer system and disclosing information in the system to third parties or using such information except for legitimate business purposes, the Nosal court held that the current employees exceeded their authorized access when they accessed information from the company's system and sent it to the former employee in violation of that prohibition. Because the former employee was charged with aiding and abetting and conspiring with the current employees to violate the CFAA, the court ruled that both he and the employees could be held criminally liable.

Courts have, in many cases, been reluctant to apply CFAA liability to employees who access company information prior to their departure for competitive purposes, likely due to the prospect of criminal liability. As a result, where an employer's acceptable use policy lacked sufficient clarity or did not address this issue, courts have taken the opportunity to absolve the employee of liability. A frequently cited example of this line of reasoning can be found in *LVRC Holdings LLC v. Brekka*, a case also decided by the Ninth Circuit less than two years prior to Nosal. In that case, a telecommuting employee frequently emailed company records to his personal email account for purposes of continuing work at home.

The employer did not prohibit this activity, either verbally or in a written policy. As a result, the court declined to find the employee liable after he emailed confidential company materials to himself and his wife, including the administrative password to the employer's email system and patient lists, allegedly for use in competitive behavior once his employment ended. The employer argued this activity was done to further the employee's own interests, and so was taken "without authorization" in violation of the CFAA. The court disagreed, finding that the extent of the employee's authorization depends on "actions taken by the employer" and is not determined in light of the loyalty or duties of the employee.

With *Nosal* and *Brekka*, the Ninth Circuit has provided employers with a roadmap to preserve CFAA claims when employees abuse their authorization to access protected information for inappropriate purposes. The following tips are based on these cases and similar decisions, as well as practical advice we have provided to clients on this issue:

- Ensure that computer use policies and contractual agreements contain clearly delineated, conspicuous restrictions regarding use of information systems for unauthorized purposes. Those purposes must be articulated as specifically as possible, rather than relying on broad bans on "unauthorized use" or "competitive purposes."

- Prohibitions on unauthorized access and use should be repeated and reinforced through training, security reminders, and warnings presented at each log in.

- Supervisors should be cautioned against undercutting these policies with inconsistent statements or behaviors (such as tolerating employees emailing protected information to their personal accounts if that activity is inconsistent with company policy).

- Policies regarding appropriate access and use should be expressly extended to employees' use of personal devices for business purposes if the employer allows business use of personal devices.
- Policies should clearly articulate that an employee's authorization to access company information or systems ends upon termination, particularly if there have been past difficulties effectively ending technical access upon termination.

Other considerations may be relevant depending on the employer's circumstances and the authorized activities of their workforce. The greater the clarity provided to employees regarding the scope of their authorization to use company information, the more likely a CFAA will be successful if and when that scope is exceeded.