ROGERS & HARDIN

Client Advisory
The Computer Fraud and Abuse Act

Contact Information
Katherine L. D'Ambrosio
kdambrosio@rh-law.com
S. Gardner Culpepper
gculpepper@rh-law.com
Daniel D. Zegura
dzegura@rh-law.com
Austin J. Hemmer
ahemmer@rh-law.com

Protecting Information from Departing Employees: The Computer Fraud and Abuse Act

When an employee leaves her job, there is always a risk that she will take confidential company information with her. Given the possibility of significant lay-offs in the wake of the coronavirus, employers should carefully consider steps they can take now to protect their trade secret and confidential business information. While trade secret statutes provide an important layer of protection, employers should also consider whether they can bring a successful claim under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"). The CFAA offers broad protection because it applies to *all* company information, regardless of whether it qualifies as a trade secret. Therefore, if you discover that a current or former employee has accessed company computers to steal company information, you should consider whether bringing a CFAA claim is an option.

The CFAA

The CFAA prohibits individuals from accessing a computer without authorization (or in excess of their authorized access) to obtain information. The statute provides for civil and criminal penalties. In the civil context, a plaintiff can obtain injunctive relief as well as monetary damages. Although Congress primarily enacted the CFAA to address computer crimes such as hacking, employers can bring civil claims against former employees under certain circumstances.

A key issue in CFAA cases is whether the defendant accessed the computer in question "without authorization" or "exceed[ed]" his "authorized access." Because most employees will have access to the company's computer systems, whether you can successfully bring a CFAA claim against a departing employee often depends on how the courts in your jurisdiction have answered the following question: Does accessing information for an unauthorized ***purpose*** constitute "exceed[ing] authorized access"—for example, when an employee accesses data she is authorized to access but for purposes contrary to the employer's interests? The courts are split on this issue. *See United States v. Valle*, 807 F.3d 508, 524 (2d Cir. 2015) (noting circuit split). Adopting the broader view, the Eleventh Circuit has held that an employee exceeded his authorized access when he violated a policy prohibiting employees from obtaining information from databases without a business reason. *See United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010). Review the case law in your governing jurisdiction to determine whether a CFAA claim is viable under the circumstances.

The following checklist offers some steps potential CFAA litigants can take both before and after a breach to maximize their chances of success.

1. Clearly communicate the limits on employee access to company information. Employers should have computer and internet access and use policies (as well as confidentiality agreements) that restrict the permissible access to and use of sensitive information. These policies should specifically prohibit the use or

disclosure of sensitive information for any purpose other than company business. Access to especially sensitive information should be restricted to select groups of employees on a "need to know" basis. These access policies should be regularly communicated to employees via training sessions and written reminders.

2. Promptly terminate access of departing employees. When an employee leaves, immediately terminate computer access and deactivate all passwords. If there is a legitimate suspicion of misconduct or if the departing employee had access to the company's most sensitive information, conduct a prompt forensic investigation (and preserve any forensic evidence). And, if any misconduct is discovered, document the date of discovery.

3. Determine the scope of "loss." You must incur a "loss" of at least $5,000 in order to bring a CFAA claim. Recoverable losses include *reasonable* costs incurred in responding to the offense, conducting a damage assessment, or restoring any data or information altered by the employee. The cost of responding to an offense may be recovered even if the company ultimately finds that the offense didn't cause any damage to its computer systems. Companies may also recover damages (such as lost revenue) incurred because of an "interruption of service." However, lost revenue related to misappropriation of trade secrets or confidential information is generally not recoverable.

4. Track all costs related to the investigation and response. Although recoverable losses will ultimately depend on the law in the governing jurisdiction, companies should document all costs incurred in responding to the offense, including internal resources (such as employee time) spent investigating the offense and payments to outside consultants. Legal fees for time spent investigating the breach and otherwise responding to the offense (such as time spent on demand letters or negotiating with the offender regarding destruction of data) may also be recoverable.

Additional Avenues for Relief

Don't forget about state laws that protect companies against computer crimes. For example, the Georgia Systems Computer Protection Act, O.C.G.A. § 16-9-90, *et al.*, penalizes computer theft and computer trespass—*i.e.*, using a computer "without authority" to take or delete information. *Id.* § 16-9-93(a)–(b). And, unlike the CFAA, the Georgia statute expressly permits the recovery of lost profits (as well as reasonable costs of investigation). However, state law remedies for computer claims related to the misappropriation of proprietary information may be preempted by other laws, such as state trade secret statutes.

* * *

Employers should take time now to shore up protection against the possibility of theft of information by departing employees. Depending on the law in your jurisdiction, a CFAA claim may be one option to combat such conduct.

This release has been prepared by Rogers & Hardin for informational purposes only and should not be considered as legal advice. This material may also be considered attorney advertising under court rules of certain jurisdictions.