

## Keep Honest People Honest With The Computer Fraud And Abuse Act

**GRAYDON HEAD**  
LEGAL COUNSEL | SINCE 1871

By Jack Greiner, Co-Chair, and Lisa Caldemeyer, Member, of the Media Communications & Information Group, Graydon Head & Ritchey

In today's environment, every business, no matter its size, must take steps to protect its data. This is so for a variety of reasons. First, in an electronic world, massive amounts of information can be transferred with a mouse click. Think back to the film version of John Grisham's novel "The Firm." And once you stop chuckling over Tom Cruise's horrendous over-acting, recall the elaborate steps his character went through to copy documents that demonstrate his firm's ties to the mob. That labor intensive interaction with the Xerox machine just isn't how it's done anymore. Second, the stakes are higher when it comes to data loss. Identity theft is a real, devastating problem — devastating for the victim, and devastating to the data custodian who allows the information to leak. Third, from a competitive standpoint, confidential data concerning processes, procedures and customer information is the key asset of any business, especially in an information age. And this type of information is particularly at risk in a time where employees are more mobile, and more apt to change jobs than ever before.

Businesses can take any number of steps to protect their data. Many of the steps are practical "IT" procedures — limit the number of people who have access to sensitive information, be vigilant about updating and disabling passwords, consider truncating social security numbers so that only the last four digits are used. Some of the steps are more "legal." For example, any employees who have access to sensitive data should sign a carefully worded nondisclosure agreement that sets forth their duties with respect to the data, both during their employment and after their employment ends for any reason.

A relatively recent federal law may help. The Computer Fraud and Abuse Act ("CFAA") is a criminal statute which prohibits anyone from "knowingly, and with intent to defraud," access[ing] a protected computer "without authorization" or "exceed[ing] authorized access" to commit fraud and obtain something



of value. The statute permits a victim to bring a civil action to recover all "compensable damages" flowing from a loss caused by the violation. The CFAA defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of an interruption of service."

Because the CFAA is a relatively new statute, courts are still determining its parameters. One area that has divided the courts is the extent to which the CFAA applies to employee data theft. In several cases, employers have argued that the CFAA applies where an employee accesses confidential information and uses that information in a new job. Not all courts have agreed. Some have found the CFAA inapplicable because at the time the employee accessed the data, he was authorized. Others have found that where there was no "interruption of service" there was no "loss."

In a more recent case, however, a Louisiana court provided some clarity. There, the court ruled that the CFAA's provision permitting recovery of "compensable damages" means all losses suffered from a violation, including lost revenue. Service interruption is not required. The court also included reasonable forensic costs as compensable losses under the CFAA.

The court felt that accepting defendant's contention that an interruption of service was required to recover any damages would lead to an "absurd result." According to the court, "[W]hen a defendant copies unauthorized data to gain a competitive

edge, it makes no sense to limit the plaintiff's recovery when the lost revenue is a direct result of the defendant's misconduct." For this same reason, the court also permitted the recovery of the costs of investigation, finding such an expense a "clearly reasonable" form of loss under the statute.

Unauthorized use may apply to situations beyond the employment setting. A company may establish rules for downloading information from its Web site. If it does, and a visitor violates the rules in the course of downloading information, that visitor may be liable under the CFAA. The information needn't qualify as a "trade secret" to invoke the protection of the CFAA.

Because the courts have split on the appropriate reach of the CFAA, the final answer may have to wait for a ruling from the United States Supreme Court. In the meantime, though, employers can do some things to potentially take advantage of the CFAA.

The company should clearly articulate rules of data access that spell out exactly what is permitted and what is prohibited. It should also secure agreement to the rules from the employee or Web site visitor. Obtaining a signed acknowledgment from the employees is probably the most effective method, but if that is not feasible, the employee handbook should state adherence to the data authorization policy as a condition of employment. It also makes sense to have the employee acknowledge that unauthorized use would require the company to incur significant expense to address the loss of the information, including costs of investigation of the extent of the loss. To obtain acknowledgment from Web site users, terms of use, and a clicking acknowledgement should work.

It has been said that "locks don't keep crooks out, they just keep honest people honest." The CFAA is one more tool for "keeping honest people honest." Employers should make sure to use it.