Using the Computer Fraud & Abuse Act to Protect Law Firm Data
By Lori Romer Stone

March 2012

There are federal statutes that can help a law firm prosecute rogue employees, who could be taking critical data with them, or damage systems and files on the way out the door.

Think about the database of a typical law firm and what it contains: reams of confidential information about the firm, its clients, and their cases. Then imagine what would happen when an employee, who is either getting ready to take a new job in the same field or who is about to be fired, accesses that data and takes it with him. Such acts can be a nightmare for the firm in protecting its proprietary interests or recovering lost files.

Increasingly, the Federal Computer Fraud and Abuse Act of 1984 (the “CFAA,” 18 U.S.C. §1030), a statute originally enacted to criminally prosecute people who hack into computer systems of the federal government and financial institutions, is being used by employers to seek damages and injunctive relief against such employees. It took two amendments to the law, in 1994 when the civil cause of action was added, and in 1996 when the act expanded the definition of protected computers to include any computer used in interstate or foreign commerce—meaning almost all computers that access the Internet—to enable businesses to use the CFAA for private relief.

However, with courts across the country split on interpreting the statute, winning a CFAA claim against an employee is not a slam-dunk case. Moreover, with Congress holding hearings over the last two years about the intent of the law, the issue is ripe for a ruling from the U.S. Supreme Court.

To succeed in a civil action against an employee suspected of computer wrongdoing, the employer, under section § 1030(a)(2)(C), must establish that the employee a) intentionally accessed a protected computer, b) accessed the computer without authorization or exceeded authorized access, c) and that such access led to at least $5,000 in damage or loss.

§1030(e)(6) of the statute defines “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 accessor is not entitled so to obtain or alter.” But even with that definition, federal courts have split over whether Congress intended the statute to apply to alleged disloyal employees violating an employer’s terms of computer use. Uncertainty also stems from the fact that “without access” is not defined in the statute, and as such, courts have also interpreted the phrase in a variety of ways. Courts have ruled differently on whether an employee who has been authorized to access information on a computer system and
does so for a disloyal or unauthorized purpose gained access “without authorization” or whether that employee exceeded authorized access under the CFAA.

“Without authorization” is a key factor in the Ninth Circuit’s 2009 ruling in LVRC Holdings LLC v. Brekka.1 The Court held that an employee, who had unrestricted access to his company’s computers during his employment, did not violate the CFAA when he sent company information and documents to his personal e-mail. This is a split from the Seventh Circuit’s opinion three years earlier in International Airport Centers v. Citrin,2 in which the Court ruled that when an employee breaches his duty of loyalty to an employer, the employee becomes “unauthorized” to access the employer’s computer. In Brekka, the Ninth Circuit rejected the Seventh Circuit’s agency theory and instead held that that when an employer authorizes an employee with full use of its computers and doesn’t revoke such unrestricted access, the employee’s personal use of electronic files does not violate the CFAA.

The most recent case involving the CFAA, which also comes out of the Ninth Circuit, could further define what constitutes exceeding authorized access. In U.S. v. Nosal,3 the Court found that the former employee violated the CFAA by hiring his former co-workers, who still worked at the firm, to send him confidential company information to start a rival firm. The panel distinguished its holding from Brekka by explaining that in Brekka, the employee had no written employment agreement and no restrictions on access to the company computer, while in Nosal, the company had a terms of use computer policy that restricted computer use to legitimate company business. The Court held that an employee who violates such a term of use policy may be held liable for exceeding authorized access under the CFAA. The Court granted the defendant’s petition for rehearing en banc, and heard oral arguments in December 2011. The outcome of the case will hinge on whether the Court interprets the phrase “exceeds authorized access” as allowing employers to criminalize their employees’ conduct when they violate the company’s terms of use computer use policies. A ruling upholding the panel’s decision could open federal courts to a floodgate of CFAA claims from employers, who would be armed with a decision restricting how employees can use their work computers and electronic information.

In the meantime, law firms can take several steps to protect themselves from employees who might access the company’s computer system and use the data for an improper purpose:

- Hold an employee seminar to review the CFAA and explain that civil and criminal penalties will follow for unauthorized access of the company’s confidential information stored on a computer system. In Nosal, criminal charges were brought against the defendant for violating the “intent to defraud” element in § 1030(a)(4) of the CFAA by the employee’s “knowing access of electronic records for uses outside their intended purpose.”4 The threat of fines and

---

1 581 F.3d 1127 (9th Cir. 2009).
2 440 F.3d 418, 420-421 (7th Cir. 2006).
3 642 F.3d 781 (9th Cir. 2011), reh’g en banc granted 2011 U.S. App. LEXIS 21777 (Oct. 27, 2011).
imprisonment can be a strong deterrent to employees tempted to be disloyal with a few clicks of the mouse.

- Review, and if necessary, update your company’s employee policies and manual to include computer use agreements. Have employees sign an agreement to acknowledge that they understand:
  - Proprietary company information is to be used only for legitimate company business;
  - Proprietary company information is not to be sent to an employee’s non-work e-mail account; and
  - Company data is not be transferred or saved to any personal computer or storage device.
- Work with your information technology department to restrict database access only to those employees who need it on a daily basis. Establish firewalls or password-protected databases for each department in the firm.

If an employee does take proprietary company information and threatens to use it or demands payment for its return, the employer should protect itself and seek relief in the CFAA in the form of a temporary restraining order or an immediate injunction. Firms should be prepared to present evidence of the theft of the data and the extortion claim. Filing a criminal complaint with the Department of Justice or the FBI should also be considered; however, a civil action asking for immediate relief will most often provide the quickest solution to the problem. And even if an employee’s actions would not be prosecuted under the CFAA, the firm could still seek remedies in state court alleging claims such as trade secret theft, breach of employment contract, and unfair competition.

With computer technology advancing at a rapid rate and changing how business gets done, employees can take steps to protect themselves from violating the CFAA. They should not save or send any information from their employer’s computer system to a personal e-mail or thumb drive without the employer’s consent. They should thoroughly review their firm’s computer terms of use or service and understand what kinds of actions could constitute a violation. If such a policy does not currently exist at their firm, a wise employee should suggest it to their boss as a means of protecting sensitive company data and quite possibly, the firm itself. Employees should also return all computer equipment provided by their employer, with all files and information intact, upon departure from the firm.

The CFAA can be a powerful tool to prevent illegal and unlawful access to computer systems, but the upcoming decision in the *Nosal* appeal and whether other jurisdictions adopt the Ninth Circuit’s reasoning will provide a clearer indication of the extent to which employers can use the statute to seek criminal and civil penalties against misbehaving employees.

**Lori Romer Stone** is a Senior Law & Policy at the University of Maryland Center for Health and Homeland Security (CHHS). She joined CHHS in February 2008. She is now a Senior Law and Policy Analyst working with the State of Maryland’s Interoperability Program Management Office to bring statewide interoperable communications to State and local agencies.