

MARCH 16, 2006

Employers Increasingly Use the Computer Fraud and Abuse Act against Disloyal Employees

By John D. Canoni

Employers are increasingly taking advantage of new civil remedies available under the Computer Fraud and Abuse Act, 18 U.S.C. Sec. 1030 (“CFAA”). This federal law particularly applies when an employee accepts a job at another company but continues working at the current job and continues to access her/his current employer’s computer system. Both the departing employee and the new employer can be sued under CFAA if, either separately or together, they seek to gain a competitive advantage through unauthorized use of information from the current employer’s computer system.

When CFAA was passed in 1994, it covered mainly classified information on government computers. Successive amendments have greatly expanded its scope. Civil remedies were added in 1994 and, in 1996, Congress (1) extended CFAA to any “protected computer” (i.e.; any computer used in interstate or foreign commerce) and (2) removed the “unauthorized access” requirement, thereby covering company insiders in addition to outside hackers.

The courts have cooperated by giving the amended CFAA a broad interpretation. In *Shurgard Storage Centers Inc. v. Safeguard Self-Storage Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash., 2000), former Shurgard employees — while still on its payroll — used its computers to send trade secrets and proprietary information to Safeguard, the new employer they had already agreed to join. CFAA covers intentional access to a computer without authorization and obtaining information from a computer by exceeding authorized access. The former employees argued that they retained their existing authority to access Shurgard’s computer system as long as they remained its employees and, therefore, had not acted without authority or in excess of their authority. The court swiftly dismissed this argument, noting the employees’ authority to access Shurgard’s computer system evaporated when they began acting as agents for Safeguard.

CFAA covers abuse of a computer system and the data on that system. A recent decision by the Seventh Circuit reveals the act will prohibit, in Judge Richard Posner’s words, “attacks by disgruntled programmers who decide to trash the employer’s data system on the way out (or threaten to do so in order to extort payments).” In that case, an employee of International



NIXON PEABODY LLP
ATTORNEYS AT LAW

Airports Centers (“IAC”), decided to go into business for himself and, before leaving plaintiff IAC, savagely attacked IAC’s computer files. He first deleted *all* data on the laptop computer IAC provided him; not only data belonging to IAC but also data that would have revealed his improper conduct. He then installed a secure-erasure software program, making it impossible for IAC to recover any of the deleted information.

District Judge Wayne Andersen held the employee’s conduct was *not* covered by CFAA because simply erasing files was not a “transmission” under that act, *International Airports Centers L.L.C. v. Citrin*, 2005 U.S. Dist. LEXIS 3905 (N.D. Ill., 2005). The Seventh Circuit unanimously reversed, 2006 U.S. App. LEXIS 5772 (7th Cir., March 8, 2006). The Court held Citrin’s authorization to access IAC’s computer system and information ended when he resolved to destroy the files that would have incriminated him and other files that were IAC’s property. Those actions violated the duty of loyalty that agency law imposes on any employee. In addition, Citrin had transmitted a program to the IAC computer intended to cause damage to that system by preventing IAC from replacing files belonging to it that he deleted.

Other cases have sustained CFAA causes of action by employees who accessed a current employer’s computer system and sent confidential information to a new employer *before* officially leaving the current employment, *HUB Group, Inc. v. Clancy*, 2006 U.S. Dist. LEXIS 2635 (E.D. Pa., January 26, 2006); *Charles Schwab & Co. v. Carter*, 2005 U.S. Dist. LEXIS 21348 (N.D. Ill., 2005). In the *Charles Schwab* case, the departing employee believed he had the right to e-mail confidential information to his new employer because Schwab was closing the division where he worked.

CFAA covers more than the losses directly caused by the employee’s unauthorized access to the employer’s computer system. It also covers damage assessments, security update and restoration or replacement costs, as well as any revenue lost or costs incurred or other damages resulting from any impairment or interruption of service. Damages must be more than \$5,000 in any one-year period. That modest minimum should easily be reached when hiring a consultant to determine if the employer’s website is secure or compromised (see e.g., *EF Cultural Travel v. Explorica Inc.*, 274 F. 3d 377, (1st Cir. 2001).

CFAA offers employers many advantages. First and foremost, employers can bring their actions *in federal court* because CFAA bestows federal question jurisdiction. CFAA claims avoid possible restrictive state non-compete or unfair competition laws. California employers can use CFAA despite that state’s general prohibition on covenants not to compete. Second, CFAA’s focus is not on the *type* of information or data stolen but on abuse of a *computer system* to obtain that information or data. Employers can bring CFAA claims without proving the information wrongfully accessed was a trade secret constituted confidential or proprietary information or breached an employment contract, confidentiality agreement or non-compete agreement. Employers can bring CFAA actions even if they do not have any confidentiality, non-compete or trade secret agreements with the disloyal employee.

CFAA actions, of course, can be two-way streets. As with non-compete and similar agreements, the employer who brings a CFAA claim one day can have one brought against it the very next day. New employers should still take action to avoid potential CFAA claims, particularly by addressing conduct by the employee while he/she is still working for the old employer but after agreeing to join the new employer. They should remind a new employee *not* to take information from a former employer, to return all computer-generated data before starting the new job and to only bring such data along if the former employer has given its permission to do so.

CFAA is also a criminal statute. That has not stopped courts from expansively construing its key elements. The law should continue to apply broadly as future disgruntled employees conceive more imaginative computer-abuse strategies.

Employers should consider using the federal Computer Fraud and Abuse Act in appropriate situations. Damages and injunctive relief are available. Key information for CFAA suits can be obtained by the former employer's own forensic computer experts. CFAA is no longer a limited statute. Expansive court interpretations have converted it into an attractive weapon against wrongful conduct by disloyal employees.

For more information on this issue or other employment law matters, please contact John D. Canoni (at 212-940-3169 or jcanoni@nixonpeabody.com) or your Nixon Peabody attorney.

The foregoing summary is provided by Nixon Peabody for education and informational purposes only. It is not a full analysis of the matter summarized and is not intended and should not be construed as legal advice. This publication may be considered advertising under applicable laws.

If you are not currently on our mailing list and would like to receive future publications of *Employment Law Alert* or if you would like to unsubscribe from this mailing list, please send your contact information, including your name and e-mail address, to lblaney@nixonpeabody.com with the words "Employment Law Alert" in the subject line. Prior publications of *Employment Law Alert* are available on our Web site at <http://www.nixonpeabody.com>.