

WSGR ALERT

FEBRUARY 2009

RECENT COMPUTER FRAUD CASE SHOWS CONTINUED IMPORTANCE OF PROTECTING INFORMATION ASSETS AND RISKS OF LITIGATION

Theft and unauthorized access to company information by departed employees continues to be an important source of litigation and concern for employers. Last month, a federal district court held that lost revenue caused by former employees' use of an employer's proprietary information taken from the employer's computer was not recoverable under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2007) (CFAA).¹

The Computer Fraud and Abuse Act

The CFAA was first enacted in 1984 with the intention of protecting classified information on government computers and financial records and credit information on government and financial institution computers. Subsequent amendments have significantly expanded its scope, including providing a private right of action to anyone who suffers more than \$5,000 in "damage" or "loss" because of a violation of the statute. Violations of the CFAA include (i) the unauthorized access to a computer for a wrongful purpose that results in the offender obtaining something of value, and (ii) the knowing transmission of "a program, information, code, or command" that intentionally causes damage to a covered computer. Companies have successfully asserted CFAA claims in widely varying contexts, including actions involving a scraper program loaded by a competitor onto the company's computer network to obtain pricing information, a data-deletion program installed by an employee on a company laptop after

the employee decided to terminate his employment, and the harvesting of e-mail addresses in order to send unsolicited bulk email. Although several courts have permitted claims under the CFAA based on harm caused by former employees' use of information improperly obtained from their prior employers' computers, the *Andritz* court joined a growing number of courts that have narrowly interpreted the types of damages and losses recoverable under the statute.

The *Andritz* Decision

In *Andritz*, an employer brought a CFAA claim against former employees who allegedly accessed the employer's computer network without authorization and obtained files containing trade secrets for the purpose of providing the files to a new employer. The provision of the CFAA at issue, 18 U.S.C. § 1030(a)(4), generally makes it unlawful for a person to knowingly, and for a wrongful purpose, access a "protected computer" without authorization, or to exceed authorized access to such a computer, and to obtain anything of value by means of such unauthorized access. For the purposes of the CFAA, a protected computer is any computer used in or affecting interstate or foreign commerce or communication. The court dismissed the case, finding that revenues lost due to the defendants' use of the improperly obtained information to lure customers from the employer were not compensable damages under the CFAA. The statute defines the "loss" required to bring a private claim 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 interruption of service." 18 U.S.C. § 1030(e)(11). The *Andritz* court interpreted this provision narrowly, holding that the only lost revenue recoverable under the statute is the revenue lost because of an interruption in computer service.

Andritz and Protecting Information Assets

Although the CFAA can be a powerful litigation weapon, especially given its potential use to recover losses incurred in responding to theft of information from company computers, the *Andritz* and other courts' narrow interpretation of actionable losses reduces the statute's utility in the context of what is at heart an employee theft of trade secrets. The litigation itself shows the continuing tension reflected in whether or not such activities are in fact "computer crimes" or whether or not computers are merely an instrument of some other already unlawful activity.

A variety of activities may help companies manage and protect their intellectual property assets when employees depart. For example, enforceable non-disclosure and non-compete agreements with all employees who have

¹ *Andritz, Inc. v. Southern Maint. Contractor, LLC*, No. 3:08-CV-44 (CDL), 2009 WL 48187 (M.D. Ga. Jan. 7, 2009).

Continued on page 2...

Recent Computer Fraud Case . . .

Continued from page 1...

access to sensitive company information can strengthen claims. More practically, companies may want to consider how they monitor and enable access to such information and ensure that access is promptly terminated when the employee departs. Finally, the presence of or access to tools that enable analysis of user activity, including log-file management, can help employers evaluate whether or if any such unlawful access has occurred. Because employee departures often result in litigation, it is strongly advisable that a business consult with counsel experienced in these issues.

Wilson Sonsini Goodrich & Rosati can assist companies with all aspects of protecting their technology infrastructure and assets. Our attorneys routinely counsel and litigate such matters. For more information, please contact Tonia Klausner, Gerry Stegmaier, or a member of our employment law practice.



Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

This WSGR Alert was sent to our clients and interested parties via email on February 5, 2009. To receive future WSGR Alerts and newsletters via email, please contact Marketing at wsgr_resource@wsgr.com and ask to be added to our mailing list.

This communication is provided for your information only and is not intended to constitute professional advice as to any particular situation.

650 Page Mill Road
Palo Alto, CA 94304-1050
Tel: (650) 493-9300 Fax: (650) 493-6811
email: wsgr_resource@wsgr.com

www.wsgr.com

© 2009 Wilson Sonsini Goodrich & Rosati,
Professional Corporation
All rights reserved.