REVISING EMPLOYMENT AGREEMENTS AND COMPUTER POLICIES TO PROTECT CONFIDENTIAL/PROPRIETARY INFORMATION UNDER THE COMPUTER FRAUD AND ABUSE ACT

Peter Gleekel Larson • King, LLP

Your client learns that a disgruntled employee has accessed her company's computer system and pilfered proprietary business information – valuable assets such as customer lists, pricing structures and distributor or supplier data. She contacts you, explains what has occurred, instructs you to prepare a lawsuit and get into court ASAP to enjoin use of the misappropriated information based upon state trade secret law. Your response may not make her happy – that despite what her company has done to designate its information as confidential, she is not protected under state law. The reason: courts can be surprisingly restrictive in how they define trade secrets, often rejecting an organization's view as to what is, in fact, a secret.

But all is not lost. When state law fails to offer protection, Federal courts may offer remedy under the Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030). A Federal Statute Act, the CFAA was enacted in 1984 as a criminal statute to protect classified information in government computer systems. A decade later, that protection – providing both compensatory damages and injunctive relief – was extended to private civil matters (18 U.S.C. § 1030(g)) in which computers are used for interstate or international commerce or communication. While state courts considering trade secret issues focus on content, Federal courts considering CFAA fact patterns focus on access to content. As the use of computers by companies of all sizes to both conduct and record business becomes universal, the CFAA has become a potentially effective tool to protect the confidential and/or proprietary information of a business by clearly restricting employee access to computer content in writing before proprietary information is breached. Afterwards, in absence of written restrictions, court decisions show that exploiting the CFAA is potentially effective but more complex.

The *prima facie* elements of a CFAA claim under § 1030(a)(2) are: (1) intentional accessing of a computer; (2) access "without authorization" or that "exceeds authorized access"; (3) data taken from a protected computer; and (4) data taken for

commercial advantage or private financial gain where the value of the information obtained exceeds $5,000. Section 1030(g), creates a private right of action, provides a civil remedy to any person who suffers "damage or loss," and provides for compensatory damages, injunctive and other equitable relief. Section 1030(e)(8)(A) defines damage as "any impairment to the integrity or availability of data, a program, a system or information" that causes a loss of at least $5,000 in aggregate value during any one-year period. The statute of limitations is two years from the discovery of the damage.

In considering strategies around the CFAA, it is vital to remember that its focus is access to – not necessarily use of – the breached information. While Federal courts are united in their understanding that spammers, hackers, competitors and other outside infiltrators have no authority to access a company's data, their view of an employee's rights differs by Circuit. At the heart of the legal interpretation is the phrase "exceeds authorized access," which, according to the CFAA, means "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 to so obtain or alter." 18 U.S.C. § 1030(e)(6).

The Fifth, Seventh and Eleventh Circuit hold an expansive view of the phrase "exceeds authorized access" that takes into account motivation and misuse in their decisions. Under this view, employees who otherwise are authorized to access a company computer can be liable for subsequent misuse of the accessed information under general theories of agency law that recognize that an employee has no authorization to access company files or information in a manner adverse to the company. These cases hold that defendants lost their authorization to access their employer's computers when they breached a duty of loyalty to their employer, even if the employer was unaware of the breach, by accessing information for a purpose contrary to the interests of the authorizing party. *E.g: Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006); *Shurgard Storage Ctrs., Inc. v. Safeguard Self-Storage, Inc.*, 119 F. Supp.2d 1121, 1125 (W.D. Wash. 2000); *Citrin*, 440 F.3d at 420; *ViChip Corp. v. Lee*, 438 F. Supp.2d 1087, 1100 (N.D. Cal. 2006); *NCMIC Finance Corp. v. Artino*, 638 F. Supp.2d 1042, 1057 (S.D. Iowa 2009).

A different view on issue of loyalty is at the core of the more restrictive interpretation of the phrase "exceeds authorized access" that has been adopted by the Fourth and Ninth Circuits, prohibiting CFAA liability for employees who abuse otherwise legitimate access to computerized company files. By this reasoning, an employee who copies files and sends them to a competitor, for example, has not exceeded authorized access and so, regardless of motivation or misuse, is not legally liable. These cases hold that authorized access to a computer system does not "exceed authorized access" unless the authorization is actually revoked. E.g., *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133-34 (9th Cir. 2009); *Shamrock Foods Co. v. Gast*, 535 F. Supp.2d 962, D. Ariz. 2008; *B&B Microscopes v. Armogida*, 532 F. Supp.2d 744, W.D. Pa. 2007.

In a potentially troubling trend for corporations, recent case law reflects this restrictive thinking, increasingly rejecting the expansive interpretation of "without authorization." The prevailing view holds that if the defendant had some authorization to access the computer at the time the computer was accessed, then, regardless of intent or misuse, the access was authorized and not protected under the CFAA.

Nor do most courts seem willing to allow for interpretation or inference in determining what constitutes unauthorized access. In *United States v. Phillips* (477 F.3d 215, 219, 5th Cir. 2007), the court did allow room for reasonable expectations, asserting the need to "analyze the scope of a user's authorization through access of protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user." However, the more common response is expressed in *EF Cultural Travel BV v. Zefer Corp.* (318 F.3d 58, 1st Cir. 2003), which rejected a reasonable expectations test for lack of authorization. Only where authority is expressly limited by restrictions memorialized in writing have most courts been willing to enforce the CFAA finding that authorized access has been exceeded. *E.g., Cont'l Group, Inc. v. KW Prop. Mgmt., LLC*, 622 F. Supp. 2d 1357, S.D. Fla. 2009; *Modis Inc. v. Bardelli*, 531 F. Supp.2d 314, D. Conn. 2008; *Hewlett-Packard v. Byd: Sign, Inc.*, 2007 WL 275476 at *13, E.D. Tex.

In light of these restrictive rulings, the soundest approach for an employer or organization to ensure protection under the CFAA is to be able to prove limits to "authorized access." To that end, a company should be prepared to present evidence showing (a) how an employee's authority to obtain or alter information on the computer was limited, rather than absolute, and (b) how the employee exceeded the limitations in obtaining or altering the information. The most prudent manner in which to do so is to memorialize the restrictions in writing, such as by a service contract, computer access policy, website notice, confidentiality agreement, employment agreement or similar contract. Additionally, password protection is an implicit limit on access for otherwise authorized users who have not been given the password.

The importance of creating written computer access policies with clearly articulated restrictions cannot be overstated. Consider the thinking of the Ninth Circuit Court of Appeals, which was asked to examine the issue of "exceeding authorized access" under CFAA in *United States v. Nosal*, 642 F.3d 781 (9th Cir. 2011). After discussing an earlier decision in *Brekka* that an employee had not violated CFAA simply by misusing accessed information since the access had not been explicitly revoked nor was the authority to access clearly limited, it determined that the Nosal employees *had* violated CFAA. The difference: because Nosal had clearly defined restrictions on access/use, its employees had *knowingly* exceeded their authorized access.

The take away for savvy employers is to leave nothing unstated, assume nothing is self-evident; just because an act of misappropriation defies common sense doesn't mean it defies the law. It's critical to expressly prohibit any employee, independent contractor or other individual who has authorization to access a computer for legitimate business reasons from accessing the computer for any improper purpose. Clearly written and imparted instructions that computer access is granted, such as "strictly for business use" and "to be used solely for the organization's business purposes," or similar restrictive language provide an organization with the best evidentiary foundation to protect and enjoin the use of its proprietary/confidential information. That way, even if the proprietary/confidential data is not officially a trade secret, the CFAA will make sure it's nobody else's business.

Peter Gleekel is a commercial litigator at Larson • King, LLP with more than 30 years of jury and bench trial experience in federal and state courts throughout the nation. He serves as lead counsel and strategist for international, national and local clients, with particular expertise in complex corporate ownership and governance disputes, and intellectual property litigation.