Protecting Proprietary Information and Trade Secrets in North Carolina: The Applicability of the Computer Fraud and Abuse Act and the North Carolina Trade Secret Protection Act

For companies, protecting proprietary information is often a top priority, especially when that information is at the core of a company’s business model. It becomes even more important when employees move on to other companies, and sometimes competitors. Although employment agreements may provide some certainty in these circumstances, they can only provide so much protection. In addition to trade secret protection under state law, employers have found success within federal law for protecting such information.

The federal Computer Fraud and Abuse Act (CFAA) is primarily a criminal statute used to combat hacking. A.V. ex rel. Vanderhye v. iParadigms, LLC, 562 F.3d 630, 645 (4th Cir. 2009). The CFAA also provides a civil cause of action for a private litigant who has suffered damage or loss under the statute. 18 U.S.C. § 1030(g). In recent years, employers have used the CFAA to bring claims against former employees for unauthorized use of and access to the employer’s internal networks and confidential information. Employers are fond of using the CFAA as a basis for these claims as there is nothing within the CFAA that requires the improperly accessed information to be a protectable trade secret or even proprietary.

The CFAA provides that individuals may be liable if they “intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[ ] . . . information from any protected computer.” 18 U.S.C. § 1030(a)(2)(C). Likewise, the CFAA covers one who “knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value.” 18 U.S.C. § 1030(a)(4). These provisions allow employers to pursue former employees who improperly obtained proprietary information before moving on to a new company.

The CFAA’s reach, however, is now questionable in the Fourth Circuit after its decision in WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012). This article examines the Fourth Circuit decision and how it contrasts with other circuits on the applicability of the CFAA. Next, it outlines basic North Carolina trade secret law and some key issues to consider in obtaining trade secret protection. This article concludes with some practical implications for those attempting to protect proprietary information through both the CFAA and North Carolina law.

WEC Carolina Energy v. Miller

In Miller, WEC Carolina filed suit against a former employee, Mike Miller, for violations of the CFAA and other various state causes of action. WEC also brought suit against Miller’s assistant and his new employer, a WEC competitor called Arc Energy Services. While Miller was employed at WEC, he was given a company laptop and access to the company’s intranet and internal documents, which contained confidential and valuable company data.

Miller resigned from WEC and joined Arc Energy, bringing his assistant along with him. WEC alleged that before he left the company, Miller downloaded several confidential and restricted documents and e-mailed them to his personal e-mail account. The company had several security policies in place, including the prohibition of misuse of company information by way of downloading that information to a personal computer.

Further, WEC alleged that weeks later Miller made a sales pitch to a potential client on behalf of Arc Energy. WEC alleged that in this presentation, Miller used the confidential information he obtained from WEC, and as a result, Arc Energy was awarded the project. WEC brought suit asserting several causes of action including misappropriation of trade secrets under state law and the CFAA claim.

The key question for the court was whether the use of information in violation of the policy, but which was obtained from a computer that Miller was authorized to access, constituted a violation of the CFAA. Specifically, whether Miller acted “without authorization” or whether he “exceed[ed] authorized access” pursuant to the CFAA in procuring and using WEC’s proprietary information.

The Fourth Circuit first noted that “an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer.” The court likewise held that an employee exceeds authorized access when he has approval to access a computer or network, but uses that access to obtain information that extends beyond the bounds of his approved access.

Importantly, the court also held that the question of whether an employee acted “without authorization” or exceeded his or her access” does not look to the improper use of the information. In other words, if Miller was originally allowed to access the information at issue, then his subsequent use of that information would be irrelevant for CFAA purposes.

The complicating factor, however, is that WEC alleged that Miller and his assistant obtained the information by downloading it to a personal computer in violation of company policy. WEC argued that accessing this information from his personal computer was a violation of company policy; therefore, Miller’s conduct was “without authorization” as defined in the CFAA.

The court disagreed, noting the ambiguities in the statute. As the CFAA provides for criminal penalties, the Fourth Circuit invoked the rule of lenity, and chose to interpret the statute more narrowly. It
Protecting, continued from page 15

held that the CFAA simply prohibits obtaining or altering information that an individual lacked authorization to obtain or alter in the first place. To hold otherwise, the court noted, would be to punish an employee with good intentions who downloads information to his personal computer so that he may work at home and make progress toward his employer’s goals.

The court further rejected an interpretation of a cessation-of-agency theory within the CFAA. Put simply, the idea is that once an employee uses his authorized access for a purpose contrary to an employer’s interests or policy, then that employee’s access is “without authorization.” Such a rule, the court held, would render employees without authorization instantly when they checked the score of a sporting event or the latest Facebook posting. Although an employer may decide to rescind authorization for such behavior, the court held that Congress did not likely intend for “the imposition of criminal penalties for such a frolic.”

Here, Miller was authorized to access the information at issue. WEC highlighted that fact when it alleged that he had access to all networks and servers, and that he had access to “numerous confidential and trade secret documents.” The court held that although Miller may have misappropriated the information, he did not access a computer without authorization or exceed his authorized access. As such, WEC failed to state a claim for relief under the CFAA, and was forced to pursue its state law claims.

The CFAA Circuit Split

Several circuits have analyzed the practice of using the CFAA in employment disputes. The Fifth, Seventh, and Eleventh Circuits have interpreted the CFAA more broadly and held that employees may be liable when they act against the employer’s interest and violate the company’s computer and data use policies. U.S. v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding employee violated CFAA when he accessed personal information for nonbusiness reasons); U.S. v. John, 597 F.3d 263, 273 (5th Cir. 2010) (holding that when an employee knows the purpose for which she is accessing information is both in violation of employer policies and part of an illegal scheme, it is proper to conclude she has exceeded authorized access within the meaning of the CFAA); Int’l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (noting that when employee breached his duty of loyalty, the agency relationship was terminated along with the authority to access the employer-provided laptop).

Other circuits, conversely, have interpreted the CFAA more narrowly. Decisions in the Second and Ninth Circuits have focused on the access versus use distinction. See U.S. v. Nosal, 676 F.3d 854, 864 (9th Cir. 2012); Orbit One Communs. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) (“The CFAA expressly prohibits improper ‘access’ of computer information. It does not prohibit misuse or misappropriation.”)

In Nosal, the Ninth Circuit held that a group of employees at an executive search firm did not violate the CFAA when they retrieved confidential information through their company user accounts and transmitted them to a competitor and former employee. Similar to the Fourth Circuit in Miller, the Fourth Circuit held that the CFAA fails to provide a remedy for misappropriation of trade secrets and for violations of a use policy when the employee was authorized to access such information.

Despite this circuit split, the Department of Justice decided on August 2, 2012, that it would not seek Supreme Court review in Nosal. David Kravets, DOJ Won’t Ask Supreme Court to Review Hacking Case, Wired, Aug. 10, 2012 (available at http://www.wired.com/threatlevel/2012/08/computer-fraud-supreme-court). Thus, counsel must be aware in examining the CFAA’s applicability to an employment dispute which law and jurisdiction will be applicable.

North Carolina Trade Secret Law

In Miller, WEC was forced to rely on state trade secret and misappropriation laws to protect its confidential information. In North Carolina, the North Carolina Trade Secret Protection Act (NCTSPA) governs trade secret issues, and will be at the heart of any dispute where an employee is alleged to have misappropriated trade secrets or confidential information.

Whether specific information constitutes a trade secret is generally a fact-specific inquiry. The NCTSPA defines a trade secret as business or technical information that “derives independent actual or potential commercial value from not being generally known or readily ascertainable through independent development or reverse engineering by persons who can obtain economic value from its disclosure or use; and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.” N.C.G.S. § 66-152(3).

In interpreting the statute, North Carolina courts have fashioned six factors to determine whether information is a trade secret: (1) the extent to which the information is known outside the business; (2) the extent to which it is known to employees and others involved in the business; (3) the extent of measures taken to guard the secrecy of the information; (4) the value of information to business and its competitors; (5) the amount of effort or money expended to protect the secret; and (6) the ease or difficulty with which the information could properly be acquired or duplicated by others. Area Landscaping, L.L.C. v. Glaxo-Wellcome, Inc., 160 N.C. App. 520, 525, 586 S.E.2d 507, 511 (2003); Combs & Assoc’s v. Kennedy, 147 N.C. App. 362, 369–70, 555 S.E.2d 634, 640 (2001); State ex rel. Utilities Comm’n v. MCI Telecomms. Corp., 132 N.C. App. 625, 634, 635, 514 S.E.2d 276, 283 (1999).

Generally, one of the most important factors in determining whether information constitutes a trade secret is whether an organization took proper steps to secure the information at issue. For example, providing confidential information to a customer and not limiting the use of such information would not be reasonably maintaining the secrecy of that information. Area Landscaping, 160 N.C. App. at 526, 586 S.E.2d at 512; see also Combs, 147 N.C. App. at 370, 555 S.E.2d at 640 (holding that a letter containing confidential information plus the public availability of business records did not constitute reasonable maintenance of secrecy). Accordingly, for organizations seeking trade secret protection, it is imperative that they take proper steps to secure the secrecy of the information, both externally and within the organization.
In dealing with disputes between former employees and their employers, parties should be aware of the doctrine of inevitable disclosure. The doctrine of inevitable disclosure applies "when an employee who knows trade secrets of his employer leaves that employer for a competitor and, because of the similarity of the employee's work for the two companies, it is 'inevitable' that he will use or disclose trade secrets of the first employer." Analog Devices, Inc. v. Michalski, 157 N.C. App. 462, 470 n.3, 579 S.E.2d 449, 455 n.3 (2003).

In determining when to apply the doctrine, North Carolina courts have looked to several factors including: (1) any circumstances of bad faith or underhanded dealing; (2) the competitor's comparable level of technical knowledge and achievement; (3) the type of training received and the similarity between the employee's former and current position; (4) the value of the information; and (5) the degree of particularity in which the trade secret was defined. Merck & Co. v. Lyon, 941 F. Supp. 1443, 1459–60 (M.D.N.C 1996); FMC Corp. v. Cyprus Foote Mineral Co., 899 F. Supp. 1477, 1483 (W.D.N.C 1995); Analog Devices, 157 N.C. App. at 468, 579 S.E.2d at 453; Travenol Labs., Inc. v. Turner, 30 N.C. App. 686, 693, 228 S.E.2d 478, 483, 484 (1976).

As in defining a trade secret, determining whether inevitable disclosure applies is generally a fact-specific inquiry. Because these issues deal with employee mobility, however, courts may focus more heavily on an employee's skills. North Carolina has been reluctant to apply inevitable disclosure in cases where the skills learned were not specific to the processes used by a former employer; instead they were general skills and knowledge that comes from working within an area for years. Analog Devices, 157 N.C. App. at 471, 579 S.E.2d at 455. Therefore, an employer looking to assert inevitable disclosure must be aware that, especially in uncertain economic times, a court will be reluctant to limit the mobility of employees based on general skills or knowledge they may have accumulated with that employer.

**Practice Implications**

As the Fourth Circuit noted in Miller, this decision "likely will disappoint employers hoping for a means to rein in rogue employees." This will indeed make it difficult for employers to get into federal court without diversity jurisdiction unless there is also another federal claim. That does not mean, however, employers are powerless.

Although a company data policy is not enough in and of itself to have a claim heard under the CFAA in the Fourth Circuit, it is still required and is a good business practice regardless. Such a policy may include restrictions of computer use to authorized work activities only, prohibition against distributing company files to third parties, prohibition on the use of electronic storage devices and requirements that all company data and hardware be returned to the employer upon termination.

The most important policy, at least for CFAA purposes, would cover how much access is granted to each employee. The most important and prized company data should only be accessible by those employees who absolutely require it. Likewise, employees at all levels should only have access to the specific networks and data which they require for their specific job. Having such a policy in place would ensure that if employees do misappropriate data, they may be liable under the CFAA if they exceeded their granted authority.

On the actual information front, the key to securing trade secret protection is ensuring that proper security measures are in place. The need-to-know network access limitations are equally applicable here. Poor security measures, whether they be internal or external, will cut against a finding of trade secret protection.

Finally, in a dispute over trade secrets in a subsequent employment context, it is important to be aware of the doctrine of inevitable disclosure. When an employee leaves an employer for a competitor to serve an identical role, the former employer may argue that it is inevitable that the employee will disclose trade secrets. If advancing such an argument, however, that employer must be aware of courts' reluctance to restrict employee mobility. Although the CFAA's applicability has been limited in North Carolina, coupled with North Carolina trade secret law and proper security measures, employers have the ability to protect their most prized information.

**Christiaan Mazza** is a litigation associate in the Raleigh office of McGuireWoods LLP.

---

**The Liberty Garden**

The Liberty Garden continues to serve as a restful spot for all of us in and around the Bar Center. The garden is frequently used for gatherings and ceremonies, a quiet spot to reflect on a meeting, or take a quick break. New Liberty Funds are being added to the Wall of Honor, and we encourage you to consider the Lake View Plaza, where engravable pavers are in place to honor either an individual or a law firm.

Fully tax-deductible contributions entitle donors to a paver that will be a permanent part of the Bar Center. Pavers are 12” x 12”, and are available from $250 to $1,500 in one total payment. Visit www.ncbar.org/development for additional information, or contact Tom Hull, director of development via email (thull@ncbar.org) or by phone (919.677.0561 or 800.662.7407).