Employer Update

Weil

February 2018

Access v. Use:

The CFAA in the Age of the DTSA

By Jeffrey S. Klein, Nicholas J. Pappas, and Thomas McCarthy

In This Issue

Since its introduction in May 2016, the Defend Trade Secrets Act (the "DTSA") has captured the focus of employers as the foremost source of statutory protection against trade secret misappropriation, leading many employers to revise separation and confidentiality agreement templates and rework employee policies to include language specific to the statute. Somewhat forgotten in this focus on the DTSA, however, has been the Computer Fraud and Abuse Act (the "CFAA").

Once the only reliable statutory argument for federal-question jurisdiction in a trade secret dispute, the CFAA now acts as a complement to the DTSA by protecting sensitive information from a different perspective. This being said, several circuits are split on the scope of the protections afforded to employers under the CFAA, limiting the statute's effectiveness in certain jurisdictions. Even so, employers in all jurisdictions should not forget the CFAA when considering the litany of available remedies to protect sensitive information from misappropriation or dissemination, as well as when shaping personnel policies.

Background

The CFAA was originally enacted as the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, and was initially directed at protecting classified information and financial records contained on computers belonging to the government and to financial institutions. Congress then passed the Computer Fraud and Abuse Act Amendments of 1994, expanding the scope to cover "protected computers" used in interstate commerce, and creating a private right of action. But not until 2000 did the statute begin to be applied to trade secret claims. *See, e.g. Shurgard Storage Ctrs, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Washington 2000).

The CFAA imposes civil liability on any person who "intentionally accesses a computer without authorization" or "exceeds authorized access" and, in doing so, accesses or obtains information from any protected computer. *See* 18 U.S.C. §§ 1030(a)(2), 1030(a)(4), 1030(a)(5)(B)-(C). The term "without authorization" is undefined, but the CFAA defines "exceeds authorized access" as "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter." 18 U.S.C. § 1030(e)(6).

The language of the CFAA places the focus on how the individual *accessed* the information, rather than what the individual did with the information once accessed. This is in stark contrast to the DTSA, which provides a civil right of action to "[a]n owner of a trade secret that is *misappropriated*" (emphasis added). 18 U.S.C. § 1836(b)(1). Misappropriation, as defined under the DTSA, requires "acquisition of a trade secret by another by a person who knows or has reason to know that the trade secret was acquired by improper means," or "disclosure" or "use" of a trade secret that was acquired by improper means. 18 U.S.C. § 1839(5). The DTSA also applies to threatened misappropriation when a plaintiff is seeking injunctive relief. *See* 18 U.S.C. § 1836(b)(3)(A).[1]

CFAA Circuit Split

As one might guess from the wording of the CFAA, there has been significant litigation surrounding the interpretation of the phrases "without authorization" and "exceeds authorized access." This has led to a split among the circuit courts regarding what conduct constitutes a violation of the CFAA.

Expansive View

In *U.S. v. Rodriguez*, the Eleventh Circuit considered the case of a former employee of the Social Security Administration who had accessed the personal records of 17 different individuals for nonbusiness reasons while still employed by the SSA. 628 F.3d 1258 (11th Cir. 2010). The defendant argued that he had not violated the CFAA because when he accessed the personal records of the individuals, he was authorized to access the database and the information contained therein, and therefore did not "obtain or alter information in the computer that [he was] not entitled to obtain or alter." *Id*. The Eleventh Circuit disagreed, holding that "Rodriguez exceeded his authorized access and violated the [CFAA] when he obtained personal information for a nonbusiness reason" in violation of an established SSA policy. *Id*.

Other circuits have similarly held that violation of an employer's use policy constituted unauthorized access under the CFAA. In *U.S. v. John*, a Citigroup employee accessed and copied information pertaining to corporate customer accounts and provided the information to a relative that would then incur fraudulent charges. 597 F.3d 263 (5th Cir. 2010). The Fifth Circuit held that evidence had established that Citigroup had a policy prohibiting misuse of the company's internal computer systems and confidential information, and therefore the defendant had exceeded his authorized use when she accessed the information with the express purpose of facilitating fraud. *Id.* The First Circuit held in *EF Cultural Travel BV v. Explorica, Inc*. that an executive violated the CFAA by providing confidential information to third parties in violation of a company policy. 274 F.3d 577 (1st Cir. 2001). In *Int'l Airport Ctrs., LLC v. Citrin*, the Seventh Circuit held that when an employee of a real estate business deleted data regarding potential acquisition properties and proof that he had engaged in improper conduct from his company laptop, the destruction of information breached the defendant's duty of loyalty and therefore terminated the employee's authorization to access the computer. 440 F.3d 418 (7th Cir. 2006).

Restrictive View

In contrast to the First, Fifth, Seventh, and Eleventh Circuits, other circuits have held that so long as an employee is authorized to access and obtain certain information, their later misuse of that information does not constitute a violation of the CFAA. In *U.S. v. Nosal*, shortly after leaving an executive search firm, a former employee convinced former colleagues who were still working for the firm to help him start a competing business. 676 F.3d 854 (9th Cir. 2012). The accomplices used their log-ins to download client information and send it to the defendant in violation of a policy prohibiting the disclosure of confidential information. *Id.* The Ninth Circuit held that these activities did not constitute a violation of the CFAA because the accomplices were authorized to access the information, even if their subsequent use of the information violated the employer's policies. *Id.* The Ninth Circuit stated their belief that a broader interpretation of the statute would expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions, no matter how minor the violation. *Id*.

The Second and Fourth Circuits have adopted similar interpretations. In *U.S. v. Valle*, a police officer was charged with using his access to criminal databases to conduct a search for an individual with no law enforcement purpose. 807 F.3d 508 (2d Cir. 2015). The Second Circuit cited legislative history that it believed showed the statute was geared towards hacking and held that the defendant's subsequent misuse of information did not render his access to the information unauthorized. The Fourth Circuit joined the Second and Ninth Circuits in *WEC Carolina Energy Solutions LLC v. Miller*, holding that improper use of information validly accessed did not qualify as "unauthorized access" or "exceeding authorized access" within the meaning of the statute. 687 F.3d 199 (4th Cir. 2012).

District Courts in Undecided Circuits

Some district courts have trended towards the more restrictive view. In *Central Bank & Trust v. Smith*, the District of Wyoming held that district courts in the Tenth Circuit have universally adopted the more restrictive view espoused by the Second, Fourth, and Ninth Circuits. 215 F.Supp.3d 1226 (D. Wyoming 2016). The District Court for the District of Columbia recently held similarly, stating that while it recognizes that the statutory definition of "exceeds authorized access" is "not crystal clear," it believed that the Second, Fourth and Ninth Circuits have identified "the more persuasive reading of that phrase." *Hedgeye Risk Management, LLC v. Heldman*, Case No. 16–935 (RDM), 2017 WL 4250506 (D.D.C. September 23, 2017); *See also Cranel Inc. v. Pro Image Consultants Group*, LLC, 57 F. Supp. 3d 838 (S.D. Ohio 2014) (once an employee is granted "authorization" to access an employer's computer and the confidential information therein, a subsequent misuse of the information does not violate the CFAA); *Sebrite Agency, Inc. v. Platt*, 884 F. Supp. 2d 912 (D. Minn. 2012) (the misappropriation of confidential information stored on a computer to which the defendant has authority to access does not give rise to liability under the CFAA).

Precedent in the Third Circuit has been more mixed. The Western District of Pennsylvania held in *USG Insurance Services, Inc. v. Bacon* that an employer failed to state a claim under the CFAA where the employer alleged that the defendant had accessed confidential data with the intention of soliciting business from the plaintiff's clients on behalf of his new employer, because the employer did not plead that the employee accessed or altered any information which he was not allowed to access or alter while employed. Case No. 2:16-cv-01024, 2016 WL 6901332 (W.D.P.A., November 22, 2016). A recent opinion in the District of New Jersey held differently, denying a motion to dismiss where the employer alleged that a group of former employees accessed and obtained confidential information from the employer's computer systems in violation of company policies with the intention of soliciting the employer's other employees. *Chubb Ina Holdings Inc. v. Chang*, No. CV 16-2354-BRM-DEA, 2017 WL 499682 (D.N.J. Feb. 7, 2017).

Effective Use of CFAA Protections

In contrast to the DTSA, there are no specific disclaimers or other language that an employer must use in its agreements or policies in order to take full advantage of the protections of the CFAA. However, employers may wish to cover certain themes and topics in their policies, procedures, handbooks, and other materials that are geared towards the CFAA:

- Employers may want to consider ensuring that their information use policies prohibit unauthorized access in addition to prohibiting unauthorized use or disclosure. For example, rather than merely stating that employees are prohibited from using or disclosing confidential information for non-business purposes, an employer may also wish to state that employees are authorized to access confidential information only for business purposes.
- Employers may want to consider inserting language into employment agreements, offer letters, and/or information use policies that state that an employee's authorization to use the company's computer systems or networks is automatically revoked upon any violation of the employee's duty of loyalty, regardless of whether

the company becomes aware of the violation at that time.

- Employers may want to ensure policies are clear in prohibiting sharing of passwords, and that an individual's authorization to use company systems and networks may not be extended to any other individuals.

[1] It remains an open question whether the "inevitable disclosure" doctrine most famously discussed in *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1263 (7th Cir. 1995) is also sufficient to state a claim under the DTSA.

U.S. Supreme Court Decides the Scope of Dodd-Frank's Whistleblower Protections

By Christopher Garcia, Adam Safwat, and Agustina Berro

In a unanimous opinion issued earlier today, the Supreme Court narrowed the scope of the anti-retaliation protections of the Dodd-Frank Act, holding that the protections extend only to employees who report alleged misconduct to the SEC and not to employees who report misconduct solely to management. *See Digital Realty Trust v. Somers*, 583 U.S. ____ (2018) at 2. The decision resolves a split between the Second and Ninth Circuits, which held that whistleblower protections apply to internal whistleblowers, and the Fifth Circuit, which limited whistleblower protections to employees who have made reports to the SEC. *See Somers v. Digital Realty Trust*, No. 15-17352, 2017 WL 908245 (9th Cir. March 8, 2017); *Berman v NEO@Ogilvy LLC*, 801 F.3d 145, 151, 155 (2d Cir. 2015); *Asadi v. GE Energy* (USA), LLC, 720 F.3d 620 (5th Cir. 2013). The Court's decision is also a rejection of the SEC's long-standing position that Dodd-Frank protects internal whistleblowers.

In reaching its decision, the Court determined that the definition of "whistleblower" under Dodd-Frank "supplies an unequivocal answer" to the question of who is protected: "A 'whistleblower' is 'any individual who provides . . . information relating to a violation of the securities laws *to the Commission*.'" *Sommers*, 583 U.S. at 9 (emphasis in original). The Court further concluded that this reading of Dodd-Frank is consistent with the statute's purpose. The "core objective" of Dodd-Frank's whistleblower program is "to motivate people who know of securities law violations to *tell the SEC*." *Id*. at 11. Thus, the Act's "text and purpose leave no doubt that the term 'whistleblower'" in the anti-retaliation provision "carries the meaning set forth in the section's definitional provision." *Id*. at 12.

While today's decision limits Dodd-Frank protections for whistleblowers, companies still must be cautious in their treatment of employees who report alleged misconduct internally. Employees who report misconduct internally are still protected from retaliation under SOX. Moreover, the Court's decision makes clear that even if a company is unaware that an employee has reported to the SEC at the time it takes an adverse employment action against him or her (or is not motivated by the disclosure), the company may still be found to have violated Dodd-Frank whistleblower protections. *Id*. at 14. Accordingly, companies must continue to maintain robust anti-retaliation policies. Finally, companies should be prepared that the Court's decision likely provides incentive to whistleblowers who might otherwise be inclined merely to report internally to report to the SEC.

Employer Update is published by the Employment Litigation and the Executive Compensation & Benefits practice groups of Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

If you have questions concerning the contents of this issue, or would like more information about Weil's Employment Litigation and Executive Compensation & Benefits practices, please speak to your regular contact at Weil, or to the practice group members listed below.

Practice Group Members:

Jeffrey S. Klein
Practice Group Leader
New York
+1 212 310 8790
jeffrey.klein@weil.com

Frankfurt
Stephan Grauke
+49 69 21659 651
stephan.grauke@weil.com

London
Ivor Gwilliams
+44 20 7903 1423
ivor.gwilliams@weil.com

Miami
Edward Soto
+1 305 577 3177
edward.soto@weil.com

New York
Sarah Downie
+1 212 310 8030
sarah.downie@weil.com

Gary D. Friedman
+1 212 310 8963
gary.friedman@weil.com

Steven M. Margolis
+1 212 310 8124
steven.margolis@weil.com

Michael Nissan
+1 212 310 8169
michael.nissan@weil.com

Nicholas J. Pappas
+1 212 310 8669
nicholas.pappas@weil.com

Amy M. Rubin
+1 212 310 8691
amy.rubin@weil.com

Paul J. Wessel
+1 212 310 8720
paul.wessel@weil.com

Silicon Valley
David Singh
+1 650 802 3010
david.singh@weil.com