February 2014

Weil

Employer Update

Using the Computer Fraud and Abuse Act to Protect Confidential Information

By Jeffrey S. Klein, Nicholas J. Pappas, and Sarah Martin

In This Issue

Employers frequently seek to prevent unauthorized use or disclosure of confidential information by enforcing non-competition or confidentiality agreements against employees who resign to work for competitors. However, employers who have not entered such agreements with their employees nevertheless have available to them various state statutory and common law claims such as tortious interference, breach of fiduciary duty, civil conspiracy and unfair competition. We have previously written about the enforcement of contractual, common law and statutory methods for protecting confidential information,[1] but we have not yet specifically focused on a relatively new theory that employers are asserting in litigation with greater frequency, a federal claim under the Computer Fraud and Abuse Act (CFAA). 18 U.S.C. § 1030.

The CFAA was initially enacted in 1986 as a criminal statute, and prohibited anyone from accessing a computer system belonging to a bank or the federal government without authorization. Pub. L. No. 98-474, 100 Stat. 1213 (1986). In 1994, Congress expanded the reach of the CFAA by adding a civil remedy. Pub. L. No. 103-322 § 290001(g), 108 Stat. 1796 (1994).

The CFAA provides that anyone who "knowingly and with intent to defraud, accesses a personal computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value ... [or] intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss ... shall be punished." 18 U.S.C. § 1030(a)(4)-(5)(C). Under the CFAA's civil action, anyone "who suffers damage or loss by reason of a violation" of most of the CFAA's provisions "may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." Accordingly, an employer now has a federal cause of action against an employee who obtains information by accessing a "protected computer"[2] "without authorization" or exceeding his or her "authorized access," provided that the loss to the employer exceeds at least $5,000 in value, or if the offense causes:

(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more

individuals; (III) physical injury to any person; (IV) a threat to public health or safety; (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or (VI) damage affecting 10 or more protected computers during any 1-year period.

18 U.S.C. §1030(g). If successful, an employer may obtain both compensatory damages, injunctive relief or "other equitable relief." *Id*.

Courts disagree, however, about how broadly the CFAA, and specifically the definition of "exceeds authorized access," can be interpreted. The CFAA defines the term "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." § 1030(e)(6). The First, Fifth, Seventh and Eleventh Circuits have held that the CFAA can apply to employees who have access to a protected computer that stores their employer's confidential information but use that information for a wrongful or disloyal purpose. The Fourth and Ninth Circuits, however, have held that employees violate the CFAA only if they obtain information without their employer having given them access to the source of that information.

Courts disagree about whether a breach of a policy that permits employees to access confidential or proprietary information but forbids using that information for certain purposes (a so-called use policy) constitutes a CFAA violation.

In 2012, it appeared that the Supreme Court would resolve the conflict in the circuits when it granted a petition for certiorari in *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 207 (4th Cir. 2012), where the Fourth Circuit held that an employee who downloaded confidential and proprietary information to his personal computer, in violation of company policy, did not violate the CFAA. However, the Supreme Court recently dismissed the petition for certiorari at the parties' request. *WEC Carolina Energy Solutions LLC v. Miller*, 133 S. Ct. 831 (2013). In this article, we analyze divergent interpretations of the CFAA and offer some suggestions regarding how employers can craft their policies so as to maximize the possibility of using the CFAA to protect confidential information in the hands of departing employees.

Disloyal Access

Some courts have concluded that an employee may act "without authorization" or "in excess of authorized access" under the CFAA when he accesses confidential or proprietary information from his employer's computers that he has permission to access but then uses that information in a manner that is inconsistent with the employer's interests or in violation of contractual obligations or fiduciary duties. For example, the Seventh Circuit held that a breach of an employee's duty of loyalty can create liability under the CFAA in *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006). In that case, an employer loaned an employee a laptop, on which the employee was to record data collected in the course of his work. Before resigning to start his own business, the employee allegedly deleted all of the data on the employer's laptop, including data that he had collected for the employer's benefit. The district court dismissed the employer's suit for failure to state a claim, and the plaintiff appealed. *Id*. at 418-19. The court found that under these circumstances the employer stated a claim under the CFAA, even though the employer had given him access to the computer and authority to use the computer to collect data, as well as to "return or destroy" "confidential data" upon conclusion of his employment. The court stated that the employee allegedly had breached his duty of loyalty by destroying files that were the property of his employer, because the provision in the employee's contract permitting him to "return or destroy" confidential data was not intended "to authorize him to destroy data that he knew the company had no

duplicates of and would have wanted to have." *Id*. at 421. The court held that the employee's "breach of his duty of loyalty terminated his agency relationship ... and with it his authority to access the laptop, because the only basis of his authority had been that relationship." *Id*. at 420-21.[3] The Court of Appeals consequently reversed the lower court's dismissal, and reinstated the suit. *Id*. at 421.

Other courts have adopted a much more narrow interpretation of the CFAA than the one applied by the Seventh Circuit and have held that employees violate the CFAA only by the unauthorized access, obtainment, or alteration of information, not the disloyal misuse or misappropriation of information obtained without permission. For example, the Fourth Circuit rejected the Seventh Circuit's interpretation in *WEC Carolina Energy Solutions LLC v. Miller*. 687 F.3d 199, 203 (4th Cir. 2012). In that case, an employer had given its employee permission to access company intranet and servers as part of his employment. The employee allegedly downloaded his employer's proprietary information before resigning, and then used that proprietary information to make a presentation to the employer's customers on behalf of a competitor. The court held that liability under the CFAA was limited "to individuals who access computers without authorization or who obtain or alter information beyond the bounds of their authorized access" and that the statute could not be used as a "vehicle for imputing liability to workers who access computers or information in bad faith ..." *Id*. at 207.

Breach of a Use Policy

Courts disagree about whether a breach of a policy that permits employees to access confidential or proprietary information but forbids using that information for certain purposes (a so-called use policy) constitutes a CFAA violation. The Eleventh Circuit held that the breach of a use policy violates the CFAA in *United States v. Rodriguez*. 628 F.3d 1258, 1263 (11th Cir. 2010). In that case, a Social Security Administration (SSA) employee used his access to an SSA database to obtain personal identifying information for people he knew or their relatives. The SSA's policy prohibited employees "from obtaining information from its databases without a business reason." 682 F.3d at 1260. The employee (Rodriguez) was criminally convicted for his CFAA violation and sentenced to twelve months imprisonment. Rodriguez then appealed his conviction. The Eleventh Circuit held that Rodriguez had exceeded his "authorized access," and thereby violated the CFAA, when he obtained personal information for non-business reasons. 628 F.3d at 1263.[4]

The Fourth and Ninth Circuits have both rejected the Eleventh Circuit's reasoning. Both courts hold that the violation of a use policy does not "exceed authorized access" under the CFAA. In *United States v. Nosal*, the employer's policy specifically forbade disclosing confidential information, and the computer system warned users that the database was to be used "for business purposes only." 676 F.3d 854, 856 n.1 (9th Cir. 2012). Nonetheless, the Ninth Circuit held that an employee's violation of the company policy was not a CFAA violation. The Ninth Circuit held that the phrase "exceeds authorized access" in the CFAA "is limited to violations of restrictions on access to information, and not restrictions on its use." 676 F.3d at 863-64. The Fourth Circuit, in *WEC Carolina Energy Solutions LLC v. Miller*, forbade interpreting "exceeds authorized access" as including violation of a use policy, but stated that liability could be found for "individuals who access computers without authorization or who obtain or alter information beyond the bounds of their authorized access." 687 F.3d 199, 207 (4th Cir. 2012).

Drafting Effective Policies

Given the judicial disagreement as to the correct interpretation of the CFAA, employers should carefully consider how to craft their policies governing confidentiality and the use of computers in order to take the greatest possible advantage of the CFAA's civil provisions. Employers can maximize their ability to make use of the CFAA by drafting policies which prohibit the use of confidential or proprietary information for personal benefit, non-business purposes, or for the benefit of any third party (including a competitor). These use policies will encourage employees not to use their employer's confidential or proprietary information for their own

gain in jurisdictions where courts recognize the violation of a use policy as establishing unauthorized access under the CFAA.

Under current law prevailing in the Fourth and Ninth Circuits (or in circuits where the law surrounding the CFAA is currently unsettled), employers may not be able to rely on use policies to establish that an employee's access to a computer was unauthorized. Those employers can still use the CFAA to their advantage, however, by carefully limiting the access each of their employees has to databases or servers containing confidential or proprietary information. Employers should not grant access to the servers and databases where confidential or proprietary information can be found to employees who do not actually need confidential or proprietary information in order to perform their job duties. If employees gain access to prohibited servers or databases, they will be accessing information "without authorization," and will therefore be liable under the CFAA. In addition to limiting employees' authorized access, employers should make clear that employees have no expectation of privacy on company computers. This admonition will allow an employer to monitor its employees' computer activities, and will improve the employer's ability to determine whether an employee has exceeded his or her authorized access.

Employers also should reconsider the language in their standard contractual provisions pertaining to the use of confidential and proprietary information. Contractual provisions can help protect an employer's information where the CFAA does not. A standard confidentiality provision, for example, might specifically include data found on computers within the definition of "confidential information." A contract can also specifically forbid employees from downloading company data to personal devices, and can require employees to return all data upon the termination of their employment and to present their personal computers, cell phones or other PDA's to the company's IT department for review and removal of company data at the conclusion of employment.

Contractual provisions can help protect an employer's information where the CFAA does not.

1. Jeffrey S. Klein and Nicholas J. Pappas, *Trade Secrets and California Ban on Noncompetition Agreements*, NEW YORK LAW JOURNAL (Dec. 6, 2013); Jeffrey S. Klein and Nicholas J. Pappas, *Developments in the Law of 'Inevitable Disclosure'*, NEW YORK LAW JOURNAL (Apr. 4, 2011); Jeffrey S. Klein and Nicholas J. Pappas, *Enforceability of 'Forfeiture-For-Competition' Agreements*, NEW YORK LAW JOURNAL (Feb. 3, 2003); Jeffrey S. Klein and Nicholas J. Pappas, *Departing Employees and the Doctrine of Inevitable Disclosure*, NEW YORK LAW JOURNAL (Dec. 7, 1998); Jeffrey S. Klein and Nicholas J. Pappas, *Protecting Customer Data from Ex-Employees*, NEW YORK LAW JOURNAL (June 2, 1995).
2. A computer that "is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States" is a "protected computer." 1030(e)(2)(B).
3. *See also EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583-84 (1st Cir. 2001) (in which a former employee likely exceeded "authorized access" when he accessed a website that was open to the public, but allegedly used his former employer's confidential information to obtain greater information from the website than was available to the public).
4. *See also United States v. John*, 597 F.3d 263, 289 (5th Cir. 2010) (in which the court upheld the conviction of a Citigroup account manager who used her access to customer account information to enable her brother to incur fraudulent charges).

Pre-termination Negotiations in the UK: How to Use the New Regime When Looking to Exit an Employee

By Ivor Gwilliams and Tas Voutourides

In the last two years, there has been a fairly dramatic change to the employment landscape in the UK. During this period, the UK government has introduced a number of changes with the aim of reforming UK employment law and, in particular, reducing the number of unfair dismissal claims. These changes have included:

- Increasing the unfair dismissal qualifying period from one year to two years;
- Limiting the compensatory award cap for unfair dismissal claims to the lower of the current cap of £74,200 or one year's gross pay;
- Introducing fees in tribunals for all employment claims; and
- Establishing a new regime allowing employers and employees to participate in confidential pre-termination negotiations.

Readers of our Employer Update alert of February 2013 will already be familiar with many of the changes that have taken place to the UK's unfair dismissal rules and employment tribunal regime. In this update, we will explain how employers in the UK can use the new regime of "pre-termination negotiations" to their advantage.

Scope of Protection Available to Employers

Employers wanting to carry out pre-termination discussions with employees have to ensure that the discussions are identified as "without prejudice." This common law principle of "without prejudice" will generally prevent statements that are made in a genuine attempt to settle an existing dispute from being disclosed in any subsequent legal proceedings. The difficulty is, however, that the parties must be in a dispute before being afforded such protection. In practice, employers often hold settlement discussions before a dispute arises (i.e., before the without prejudice rule applies), and thus take the risk that the conversation will be admissible in subsequent legal proceedings. Therefore, employers have to be fairly certain that they will be able to reach an agreed settlement before embarking on purportedly "without prejudice" conversations. For this reason, the without prejudice regime, although useful, has its limitations.

Employers and employees are now able to enter into confidential negotiations with a view to reaching agreed terms on ending an employment relationship without the risk of such discussions being referred to in … unfair dismissal proceedings.

However, the introduction of the new pre-termination negotiations regime provides an additional layer of protection for employers in the UK. Employers and employees are now able to enter into confidential negotiations with a view to reaching agreed terms on ending an employment relationship without the risk of such discussions being referred to in certain (but not all) subsequent legal proceedings, namely unfair dismissal proceedings.

Unfair dismissal is a form of UK statutory protection available to employees who in most cases (from April 2012) have at least two years' service. In order to fairly dismiss such an employee, an employer will have to establish a prescribed fair reason for the dismissal and show that, under the circumstances, it acted reasonably in treating that reason as a sufficient reason for the dismissal and that it carried out the dismissal fairly. Otherwise, the dismissal will be held to be unfair. If an employee succeeds with his or her unfair dismissal claim, an employment tribunal can award an employee both a basic award and a

compensatory award. A basic award is calculated by taking into account an employee's age, years of service and average weekly wage with the award itself capped currently at £13,500. The maximum compensatory award that an employment tribunal can award an employee is currently the lower of £74,200 or 12 months' gross pay.

Employers in the UK will be able to carry out pre-termination negotiations without the risk of an employee resigning and claiming constructive unfair dismissal as long as they do not exhibit any "improper behavior." A constructive unfair dismissal is where an employee resigns in response to a fundamental breach of contract by the employer (i.e., treats him/herself as having been constructively dismissed) and brings claims for wrongful dismissal (i.e., for failure by the employer to serve the required period of notice) and unfair dismissal.

Limitations of This Protection for Employers

To obtain the protection of the new pre-termination negotiations regime, certain key conditions will need to be met. Firstly, the protection will only be in respect of "ordinary" unfair dismissal claims. Should an employee bring claims for automatic unfair dismissal (for example, whistleblowing) or any other claim, such as discrimination or breach of contract, the protection will not apply and evidence from any pre-termination negotiations will be admissible in legal proceedings unless the employer can rely on the without prejudice rule. The danger, therefore, is that should an employee bring subsequent claims, such as discrimination claims, the protection will not apply. This is a problem, as increasingly employees add additional claims, such as discrimination and whistleblowing claims, to their unfair dismissal complaints.

Secondly, as with the without prejudice principle, evidence of pre-termination negotiations may be admissible should either the employer or employee engage in "improper behavior." Improper behavior is widely defined in the Code of Practice on Settlement Agreements issued by the Advisory, Conciliation and Arbitration Service (ACAS), a body that promotes and facilitates good employment relations practice in the UK. Examples include circumstances in which employers threaten employees with dismissal prior to any disciplinary action being taken or where discriminatory comments are made. Any undue pressure on employees to accept settlement terms and other forms of victimization and harassment could also amount to improper behavior and potentially lead to claims for constructive dismissal.

There is also uncertainty surrounding the impact of pre-termination negotiations on breach of contract claims. The wording of the legislation makes it clear that in the absence of improper behavior, the details of pre-termination negotiations remain inadmissible and cannot be used by an employee to assert a fundamental breach of contract in the context of a claim for constructive dismissal. Strangely, however, pre-termination negotiations will be admissible for straightforward breach of contract claims relating to, for example, payment for the notice period. This presents a particular problem for employers looking to dismiss senior executives with long notice periods (whose contractual entitlements are more important financially than their unfair dismissal rights). As such pre-termination negotiations are admissible for the purposes of straightforward breach of contract claims, senior executives *may* be able to argue that the settlement offer or its terms amount to a fundamental breach of their employment contract allowing them to resign and treat themselves as having been constructively dismissed. The senior executive would then be able to bring a claim for the employer's failure to serve the required period of notice and also to argue that their post-termination restrictive covenants

Employers should continue to make it clear to employees at the outset of any pre-termination negotiations that the discussion is taking place on a without prejudice basis.

have fallen away and are no longer enforceable as a result of the employer's breach. This risk therefore underlines the need for employers to ensure that they communicate to employees that such discussions are also taking place on a without prejudice basis, even if such discussions may not genuinely be considered to be without prejudice until a dispute exists.

Steps Employers Can Take to Maximize the Protection Available

Employers will have to proceed with care and, to this end, there are a number of precautions they can take to ensure they are afforded as much protection as possible when carrying out such negotiations. These are set out below:

- Employers should continue to make it clear to employees at the outset of any pre-termination negotiations that the discussion is taking place on a without prejudice basis. As long as there is a dispute between the parties, this will protect the confidentiality of the negotiations should an employee bring additional claims subsequently.
- Managers who carry out such negotiations should receive prior training and be aware of what may amount to improper behavior to ensure that potentially discriminatory and other inappropriate comments are not made.
- Always allow an employee a reasonable period in which to consider any settlement terms and, if necessary, obtain advice. Do not exert undue pressure on employees to accept any terms offered.

Impact of the New Regime in Reducing the Number of Employment Claims

It is clear that this new regime of pre-termination discussions is not a panacea and so will not afford employers with a complete cloak of protection. It is still, however, a welcome development for employers, as it allows them to have honest and frank discussions with employees. This will be valuable in circumstances where, for example, no clear dispute has yet arisen between the parties but there are clear performance issues with an employee that are of concern. It is also the UK government's hope that this regime will help employers and employees to reach amicable settlements without the need to resort to litigation and thereby reduce the burden on employment tribunals. To this end, there is anecdotal evidence that suggests that the combination of the new changes introduced is already leading to a reduction in UK employment tribunal claims. Unfortunately, an unintended consequence of this is that employees are now arguably more likely to bring alternative claims, such as discrimination and whistleblowing, where an unfair dismissal claim is not possible. Finally, it remains the case in the UK that it is far easier for an employer to dismiss an employee who has not yet accrued unfair dismissal rights, provided that there are no whistleblowing or discrimination issues.

Employer Update is published by the Employment Litigation and the Executive Compensation and Employee 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 and Employee Benefits practices, please speak to your regular contact at Weil, or to the editors or practice group members listed below:

Editor:

Lawrence J. Baer lawrence.baer@weil.com +1 212 310 8334

Associate Editor:

Millie Warner millie.warner@weil.com +1 212 310 8578

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

Joanne Etherton
+44 20 7903 1307
joanne.etherton@weil.com

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

Miami

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

New York

Lawrence J. Baer
+1 212 310 8334
lawrence.baer@weil.com

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

Michael K. Kam
+1 212 310 8240
michael.kam@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