Second Circuit Decision Highlights Rift in Case Law Over When Computer Fraud and Abuse Act Can Be Used to Combat Employee Theft of Data

Kevin J. O'Connor, Esq.

With the proliferation of technology in the modern workplace, employee theft of confidential and proprietary computer data is often involved in non-compete cases. I have written extensively in prior articles on the scope of remedies available under the *Computer Fraud and Abuse Act*, 18 U.S.C. § 1030 *et seq.* ("CFAA") and its New Jersey state law counterpart, the *Computer Related Offenses Act*, N.J.S.A. § 2A:38A-3 *et. seq.* ("NJCROA"). A new decision from the Second Circuit has highlighted the significant barriers to using the CFAA in New York, Vermont and Connecticut, to deal with an employee's improper use of computer data, at least until this issue is put to rest by the United States Supreme Court or by an act of Congress. In *U.S. v. Valle*, 2015 WL 7774548 (2d Cir. Dec. 3, 2015), the Court held that it is not enough to show that an employee with authorization and login credentials to the company network misused his access in violation of a company computer use policy. Rather, an employer seeking redress under the CFAA in those states must now show that an employee did not have authorization and bypassed a technological barrier to access the information. *Valle* highlights the need for employers to revisit their technical security measures to ensure their data is safe not just from what are traditionally viewed as "hackers," but from disloyal employees as well.

BACKGROUND ON CFAA

The CFAA, a federal act, provides a private right of action to those who have suffered "losses" due to violations of the Act. *See* 18 U.S.C. § 1030(g). Section 1030(a)(2)(c) imposes liability, among other things, upon any person who intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from a protected computer. Under

the CFAA, a "protected computer" is one which, among other things, is used in interstate commerce or communication. 18 U.S.C. § 1030(e)(2)(B).

The Third Circuit in *P.C. Yonkers, Inc. v. Celebrations: The Party and Seasonal Superstore, LLC*, 428 F.3d 504, 510-511 (3d Cir. 2005), recognized the availability of injunctive relief under the CFAA, but expressly held that an employer must show more than mere unauthorized access to a computer, and must make a specific showing of a probability of success on each of the elements of its claim. *Id.* at 509. Boiler-plate allegations that an employee pilfered data by emailing confidential customer lists and other proprietary information to himself will not withstand close scrutiny at the injunction stage. *See, e.g., Trading Partners Collaboration, LLC v. Kantor*, 2009 U.S. Dist. Lexis 48195, *5 (D.N.J. June 9, 2009)(denying injunctive relief; information claimed to be proprietary was generally available in the public domain); *Joseph Oat Holdings, Inc. v. RCM Digesters, Inc.*, 2010 U.S. App. Lexis 25375, *7 (3d Cir. Dec. 13, 2010)(vacating injunctive relief where underlying decision failed to consider issue of scope of authorization).

THE CONFLICTING AUTHORITIES ON THE SCOPE AND BREADTH OF THE CFAA

The area that has generated the most uncertainty is whether, under the CFAA, an employee's act of merely misappropriating data (as opposed to the traditional "hacking") can qualify for damages where the employee "exceeded authorized access" by misappropriating data. The federal courts have not universally interpreted the CFAA the same way on this score, largely because of a general reluctance to create a private right of action under a federal statute for simple common law misappropriation. Depending upon where you sue, you could get a different result entirely. Certain courts, such as the fifth and seventh circuits, have applied agency law principles and have held that an employee is never authorized to access an employer's computer in a manner inconsistent with the duty of loyalty to the employer. Applying such a rule, the moment the employee uses the com-

puter to misappropriate proprietary information, he can be liable under the CFAA regardless of the fact that the employee had been granted such access as part of his or her duties. *United States v. John*, 597 F.3d 263, 271 (5th Cir. 2010); *International Airport Centers, LLC v. Citrin*, 440 F.3d 418, 419 (7th Cir. 2006).

In *Citrin*, where an employee erased data from company computers to cover his tracks in having formed his own business on company time and having copied data, the court held that an employee's "authorization" for purposes of the CFAA ended the moment he violated his duty of loyalty to his employer. *Citrin*, 440 F.3d at 419. The Fifth Circuit has similarly held that an employee will violate the CFAA when he or she crosses the line and misappropriates data. *John*, 597 F.3d at 271.

Other courts have taken a stricter approach and, applying the express language of the CFAA, its legislative history, and the rule of lenity in interpreting statutes with criminal applications, have held that an employee granted access to a computer cannot be held liable under the CFAA using agency principles when he merely misappropriates data for competitive purposes. *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009). Federal district courts within the Third Circuit have adopted this latter view. *See Bro-Tech Corp. v. Thermax, Inc.*, 651 F. Supp.2d 378, 407 (E.D. Pa. 2009); *Integrated Waste Solutions, Inc. v. Goverdhanam*, 2010 U.S. Dist. Lexis 127192 (E.D. Pa. Nov. 30, 2010).

Similarly, until now, the Second Circuit had not fully spoken on this issue, and lower level courts within the Second Circuit have held that the CFAA is to be narrowly construed and was never intended to prohibit employee misappropriation of data. *Jet One Group, Inc. v. Halcyon Jet Holdings, Inc.*, 2009 WL 2524864 at *5, 6 (E.D.N.Y. Aug. 14, 2009) (citing *Nexans Wires S.A. v. Sark-USA, Inc.*, 166 Fed.Appx. 559, 2006 WL 328292 (2d Cir. Feb. 13, 2006)); *see also U.S. v. Aleyni-*

kov, 2010 U.S. Dist. Lexis 92101, *14 (S.D.N.Y. Sept. 3, 2010) (providing an extensive analysis of the split between the circuits in applying the CFAA). Such cases have the effect of taking outside the statute any case where an employee merely exceeded company access in misappropriating data that he or she was otherwise authorized to work with in the course of his normal duties.

The *Valle* decision presents a fascinating factual background different from what is usually seen in cases applying the CFAA. Gilberto Valle, an officer in the New York City Police Department, was an active member of an internet sex fetish community. He connected online through his computer with others who had similar proclivities, and exchanged ideas about performing various sexual acts and acts of kidnapping and torture of women. He was also able to gain access to detailed information about women through his NYPD computer program, which he allegedly shared with others through the internet.

Valle was charged with various criminal acts, including a charge under the CFAA. He was only convicted on the CFAA charge. Despite the disturbing nature of the case, the *Valle* Court held that the defendant did not "exceed authorized access" within the meaning of the CFAA because he had been given permission by the NYPD to access its database. The Court's decision turns on whether an individual employee has circumvented a technological barrier to access information that he was never authorized to see for any purpose. The Court held that to hold as the government asked, it risked criminalizing even the most trivial violation of a company policy, such as checking one's Facebook page, making it a federal crime.

Only time will tell whether the construction of the CFAA in *Valle* will hold. Given this ruling, however, employers in this circuit (New York, Connecticut and Vermont) would be well advised to take documented, technical security measures to restrict computer access to active employees only, and compartmentalize access creating technical barriers to employees who may have ulte-

rior motives. The adoption of well written policies acknowledged by employees, along with the use of encryption and firewalls, are also advisable.

*Kevin J. O'Connor, Esq. is a shareholder with Peckar & Abramson, PC, a national law firm, and focuses his practice on EPLI , D&O, employment defense, and class action defense. He has decades of experience litigating non-competition cases, including an emphasis on computer-technology issues. He is resident at P&A's River Edge, NJ office. The views expressed herein are those of the author and not necessarily those of P&A.