

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AON RISK SERVICES NORTHEAST, INC.,

Plaintiff,

-against-

MICHAEL KORNBLAU, TYLER
WENDLEKEN, KARRYN ANGOFF, MARSH
USA INC., MARSH & McLENNAN
COMPANIES, INC., and DOES 1-50, inclusive,

Defendants.

Case No. 10 CV 2244 (RMB) (JCF)

**DEFENDANTS' MEMORANDUM OF LAW IN SUPPORT OF
THEIR MOTION TO DISMISS PLAINTIFF'S COMPLAINT**

JACKSON LEWIS LLP
59 Maiden Lane
New York, New York 10038-4502
(212) 545-4000

Clifford R. Atlas (CA 9512)
Marjorie Kaye, Jr. (MK 7141)
Ravindra K. Shaw (RS 1944)

ATTORNEYS FOR DEFENDANTS

TABLE OF CONTENTS

	<u>Page</u>
TABLE OF AUTHORITIES	ii
PRELIMINARY STATEMENT	1
STATEMENT OF MATERIAL ALLEGED FACTS	2
STANDARDS ON A MOTION TO DISMISS UNDER FED. R. CIV. P. 12(b)(6)	3
ARGUMENT	4
I. PLAINTIFF’S CLAIM UNDER THE COMPUTER FRAUD AND ABUSE ACT SHOULD BE DISMISSED AS A MATTER OF LAW.....	4
A. Plaintiff Cannot Show That The Individual Defendants Exceeded Authorized Access to Aon’s Computers, Which They Were Granted As Aon Employees.	4
B. Plaintiff Cannot Establish An Actionable “Loss.”.....	12
CONCLUSION.....	15

TABLE OF AUTHORITIES

FEDERAL CASES

	<u>Page</u>
<u>American Family Mutual Ins. Co. v. Hollander</u> , 08-CV-1039, 2009 U.S. Dist. LEXIS 16897 (N.D. Iowa Mar. 3, 2009)	6
<u>Aon Risk Servs. Northeast, Inc. v. Kornblau</u> , 10 Civ. 2244, 2010 U.S. Dist. LEXIS 38140 (S.D.N.Y. Apr. 19, 2010).....	1
<u>Ashcroft v. Iqbal</u> , 129 S. Ct. 1937, 173 L. Ed. 2d 868 (2009)	3
<u>B.U.S.A. Corp. v. Ecogloves, Inc.</u> , 05 Civ. 9988, 2009 U.S. Dist. LEXIS 89035 (S.D.N.Y. Sept. 26, 2009).....	13
<u>Bell Atlantic Corp. v. Twombly</u> , 550 U.S. 544, 127 S. Ct. 1955 (2007).....	3
<u>Black & Decker, Inc. v. Smith</u> , 568 F. Supp. 2d 929 (W.D. Tenn. 2008).....	6
<u>Brett Senior & Associates, P.C. v. Fitzgerald</u> , 06-1412, 2007 U.S. Dist. LEXIS 50833 (E.D. Pa. July 13, 2007)	6
<u>Bridal Expo, Inc. v. Van Florestein</u> , 4:08-CV-03777, 2009 U.S. Dist. LEXIS 7388 (S.D. Tex. Feb. 3, 2009)	6
<u>Civic Center Motors, Ltd. v. Mason St. Import Cars, Ltd.</u> , 387 F. Supp. 2d 378 (S.D.N.Y. 2005).....	13
<u>Clarity Servs. v. Barney</u> , 8:08-cv-2278-T-23TBM, 2010 U.S. Dist. LEXIS 32519 (M.D. Fla. Feb. 26, 2010).....	6
<u>Condux International, Inc. v. Haugum</u> , 08-4824, 2008 U.S. Dist. LEXIS 100949 (D. Minn. Dec. 15, 2008)	6
<u>Consulting Professional Resources, Inc. v. Concise Technologies, LLC</u> , 09-1201, 2010 U.S. Dist. LEXIS 32573 (W.D. Pa. Mar. 9, 2010), <u>adopted by, complaint dismissed at</u> 2010 U.S. Dist. LEXIS 31489 (W.D. Pa. Mar. 31, 2010).....	6
<u>Dedalus Foundation v. Banach</u> , 09 Civ. 2842, 2009 U.S. Dist. LEXIS 98606 (S.D.N.Y. Oct. 15, 2009)	14

<u>Diamond Power International v. Davidson</u> , 540 F. Supp. 2d 1322 (N.D. Ga. 2007).....	6
<u>International Association of Machinists & Aerospace Workers v. Werner-Masuda</u> , 390 F. Supp. 2d 479 (D. Md. 2005).....	5, 9
<u>Jet One Group, Inc. v. Halcyon Jet Holdings, Inc.</u> , 08-CV-3980, 2009 U.S. Dist. LEXIS 72579 (E.D.N.Y. Aug. 14, 2009).....	5, 7, 8, 12, 13
<u>Leocal v. Ashcroft</u> , 543 U.S. 1, 125 S. Ct. 377, 160 L. Ed. 2d 271 (2004).....	10
<u>Lockheed Martin Corp. v. Speed</u> , 6:05-cv-1580-Orl-31KRS, 2006 U.S. Dist. LEXIS 53108 (M.D. Fla. Aug. 1, 2006).....	7, 14
<u>LVRC Holdings LLC v. Brekka</u> , 581 F.3d 1127 (9th Cir. 2009)	5, 7, 10, 11
<u>Nexans Wires S.A. v. Sark-USA, Inc.</u> , 319 F. Supp. 2d 468 (S.D.N.Y. 2004), aff'd, 166 Fed. Appx. 559, 562-563 (2d Cir. 2006).....	9, 12, 13
<u>Orbit One Communications v. Numerex Corp.</u> , 08 Civ. 0905, 08 Civ. 6233, 08 Civ. 11195, 2010 U.S. Dist. LEXIS 36609 (S.D.N.Y. Mar. 10, 2010).....	5, 7, 8, 9, 10, 11
<u>Perrin v. United States</u> , 444 U.S. 37, 100 S. Ct. 311, 62 L. Ed. 2d 199 (1979).....	7
<u>Robinson v. Shell Oil Co.</u> , 519 U.S. 337, 117 S. Ct. 843, 136 L. Ed. 2d 808 (1997).....	7
<u>SecureInfo Corp. v. Telos Corp.</u> , 387 F. Supp. 2d 593 (E.D. Va. 2005)	6
<u>Shamrock Foods Co. v. Gast</u> , 535 F. Supp. 2d 962 (D. Ariz. 2008)	5, 8, 10, 12
<u>U.S. Bioservices Corporation v. Lugo</u> , 595 F. Supp. 2d 1189 (D. Kan. 2009).....	6
<u>Whitman v. American Trucking Associations</u> , 531 U.S. 457, 121 S. Ct. 903, 149 L. Ed. 2d 1 (2001).....	10

FEDERAL STATUTES

18 U.S.C. § 1030.....	1
18 U.S.C. § 1030(a)(2).....	6
18 U.S.C. § 1030(a)(2)(C)	4, 7, 9
18 U.S.C. § 1030(a)(4).....	6
18 U.S.C. § 1030(a)(5)(A)(ii)	6
18 U.S.C. § 1030(a)(5)(A)(iii)	6
18 U.S.C. § 1030(c)(4)(A)(i)(I)	4
18 U.S.C. § 1030(e)(6).....	4, 7, 8
18 U.S.C. § 1030(e)(8).....	8
18 U.S.C. § 1030(e)(11).....	8
18 U.S.C. § 1030(g).....	4, 12, 14

PRELIMINARY STATEMENT

Having recognized Plaintiff Aon Risk Services Northeast, Inc.'s ("Aon") gamesmanship and dismissed its nine state law claims, the Court has only one issue left to decide: whether a former employer can maintain a claim under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, against three former employees who were concededly granted unfettered access to its computers.¹ Defendants Michael Kornblau, Karryn Angoff, and Tyler Wendleken respectfully move to dismiss the sole remaining claim in Plaintiff's First Amended Complaint, with prejudice, pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure.²

Plaintiff's CFAA claim should be dismissed because Plaintiff's allegations fail to establish that the individual defendants exceeded their authorized access to Aon's computers. Aon acknowledges that Kornblau, Wendleken, and Angoff, who are insurance brokers, had password access to its computers but speculates that they used their access to engage in various nefarious activities for the purpose of enticing away Aon's clients. However, the CFAA prohibits unauthorized *access* to protected computers, not unauthorized *use* of those computers and the confidential information available thereon. Plaintiff's attempt to prosecute its now-dismissed state law claims for misappropriation of trade secrets and breach of contract under the guise of a CFAA claim should be rejected.

Alternatively, the CFAA claim should be dismissed because Plaintiff's allegations that the individual defendants accessed, downloaded, and attempted to delete files do not establish a cognizable "loss" under the statute.

¹ See Aon Risk Servs. Northeast, Inc. v. Kornblau, 10 Civ. 2244 (RMB), 2010 U.S. Dist. LEXIS 38140, at *2 (S.D.N.Y. Apr. 19, 2010). On or about April 23, 2010, Plaintiff re-filed its nine state law claims in the Supreme Court of the State of New York, County of New York, Index No. 601058/2010.

² A copy of Plaintiff's First Amended Complaint ("Complaint" or "FAC") is attached as Exhibit "A" to the Affidavit of Clifford R. Atlas, Esq., which has been filed herewith.

STATEMENT OF MATERIAL ALLEGED FACTS

Plaintiff Aon Risk Services Northeast, Inc. provides insurance brokerage consulting and related services. FAC, ¶ 1. Plaintiff alleges that Defendants Michael Kornblau, Karryn Angoff, and Tyler Wendleken were employed by Aon as trade credit insurance brokers, that they all resigned during the first week of February 2010, and that they were subsequently employed by Marsh USA, Inc. See FAC, ¶¶ 5, 6, 7, 24, 25.

Plaintiff alleges that it possesses information which it regards as trade secrets and confidential and proprietary information that “are known only to senior Aon executives, Aon professional staff, to the extent necessary for them to provide the services for which they were retained” and that “Aon maintains the secrecy of its trade secrets by . . . communicating policies to its employees that prohibit the use or disclosure of Aon trade secrets for non-business purposes, . . . and password protecting computer access to only Aon employees.” See FAC, ¶¶ 21, 22. Kornblau and Angoff allegedly signed agreements under which each agreed that he or she “[s]hall not, except as required in the course of employment hereunder, disclose or use during or subsequent to the course of employment, any Confidential Information which has not been publicly disclosed[.]” FAC, ¶ 28, 33. Wendleken was allegedly “required to abide by Aon policies with respect to the protection of Aon trade secrets” but Plaintiff concedes that he did “did not sign any written agreements with Aon.” FAC, ¶ 36.

Plaintiff alleges that Kornblau, Angoff, and Wendleken each “in excess of [his or her] authorization” accessed “Aon confidential and proprietary trade secret information in order to facilitate the Defendants’ competition for Aon’s trade credit clients on behalf of Marsh.” FAC, ¶ 55, 60, 62. Kornblau allegedly downloaded and deleted certain files. See FAC, ¶ 52, 53. After the individual defendants resigned, Aon allegedly arranged for a consultant to “conduct a

computer forensic analysis on the laptops assigned to the Former Employee Defendants[.]” FAC, ¶ 48.

Plaintiff readily concedes that “the Former Employee Defendants each had authority to access Aon’s protected computers, databases, and software[.]” FAC, ¶ 66. However, Plaintiff contends that this authorization was intended for purposes that it deemed proper – namely, “the limited purpose of servicing existing business, or developing additional business, for the benefit of Aon, along with other incidental use necessary for their employment with Aon.” See id. The individual defendants’ use of their access for other improper purposes was not authorized: “[t]hey were not authorized to improperly access, obtain, alter, and/or delete Aon confidential files and documents for the purpose of facilitating an unlawful solicitation of business or employees for the benefit of themselves or of an Aon competitor and to the detriment of Aon.” FAC, ¶ 67.

STANDARDS ON A MOTION TO DISMISS UNDER FED. R. CIV. P. 12(b)(6)

Although the Court must accept as true all well-pled factual allegations, a complaint must provide “the grounds upon which [the plaintiff’s] claim rests through factual allegations sufficient ‘to raise a right to relief above the speculative level’” in order to survive a motion to dismiss. Bell Atl. Corp. v. Twombly, 550 U.S. 544, 127 S. Ct. 1955, 1965, 1975 (2007). To survive a Rule 12(b)(6) motion to dismiss, the allegations in the complaint must meet a standard of “plausibility.” Ashcroft v. Iqbal, 129 S. Ct. 1937, 1949, 173 L. Ed. 2d 868 (2009) ((citing Twombly, 550 U.S. at 556-57, 570)). A claim is facially plausible “when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Id. Pleading a fact that is “merely consistent with a defendant’s liability” does not satisfy the plausibility standard. Id.

ARGUMENT

I. PLAINTIFF'S CLAIM UNDER THE COMPUTER FRAUD AND ABUSE ACT SHOULD BE DISMISSED AS A MATTER OF LAW.

As discussed below, Plaintiff's CFAA claim should be dismissed because: (1) Plaintiff admits that the individual defendants were authorized to access Aon's computers and it cannot establish that they exceeded their authorized access; and (2) Plaintiff cannot establish a "loss" within the meaning of the CFAA.

Plaintiff's Complaint does not indicate which of the many subsections of the CFAA Plaintiff is invoking. Given the Complaint's repeated references to exceeding authorization, it appears that Plaintiff is alleging a violation of 18 U.S.C. § 1030(a)(2)(C),³ which imposes liability on a defendant who "intentionally accesses a computer without authorization or *exceeds authorized access*, and thereby obtains" "information from any protected computer." See FAC, ¶¶ 51, 55, 57-62, 68; (emphasis added). To maintain a civil action, a plaintiff must also meet the jurisdictional threshold for statutorily defined "damages." The CFAA specifically provides that a civil action may only be brought if the unauthorized access causes "loss," another defined term, "to 1 or more persons during any 1-year period . . . aggregating at least \$ 5,000 in value." 18 U.S.C. §§ 1030(g), 1030(c)(4)(A)(i)(I).

A. Plaintiff Cannot Show That The Individual Defendants Exceeded Authorized Access to Aon's Computers, Which They Were Granted As Aon Employees.

Under the CFAA, "the term 'exceeds authorized access' 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 so to obtain or alter[.]" 18 U.S.C. § 1030(e)(6). The overwhelming majority of courts, including two district courts in this Circuit and the Ninth

³ In its May 5, 2010 reply letter to the Court, Plaintiff did not dispute this interpretation of its Complaint in Defendants' April 30, 2010 letter regarding this motion.

Circuit, have construed this term narrowly and refused to recognize CFAA claims alleging garden-variety misappropriation – *i.e.*, that a defendant accessed information for unauthorized or illegitimate purposes or made improper use of information that was accessed. See Jet One Group, Inc. v. Halcyon Jet Holdings, Inc., 08-CV-3980 (JS), 2009 U.S. Dist. LEXIS 72579 at *16-17 (E.D.N.Y. Aug. 14, 2009) (declining to construe “exceeds authorized access” as prohibiting “misuse” or “misappropriation” of information that is lawfully accessed because doing so would “grossly expand the statute’s reach”; granting motion to dismiss); Orbit One Communications v. Numerex Corp., 08 Civ. 0905 (LAK), 08 Civ. 6233, 08 Civ. 11195, 2010 U.S. Dist. LEXIS 36609, at *27 (S.D.N.Y. Mar. 10, 2010) (adopting narrow reading of CFAA); LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1134 n.7 (9th Cir. 2009) (“[N]othing in the CFAA suggests that a defendant’s authorization to obtain information stored in a company computer is “exceeded” if the defendant breaches a state law duty of loyalty to an employer, and we decline to read such a meaning into the statute[.]”); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 962 (D. Ariz. 2008) (“[A] violation for accessing a protected computer ‘without authorization’ occurs only when initial access is not permitted. And, an ‘exceeds authorized access’ violation occurs only when initial access to a protected computer is permitted but the access of certain information is not permitted.”; granting motion to dismiss); International Ass’n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 498 (D. Md. 2005) (“[T]o the extent that [the employee] may have breached the Registration Agreement by using the information obtained for purposes contrary to the policies established by the [employer’s constitution], it does not follow, as a matter of law, that she was not authorized to

access the information, or that she did so in excess of her authorization in violation of the CFAA.”; granting motion to dismiss).⁴

⁴ See also Consulting Professional Resources, Inc. v. Concise Technologies, LLC, 09-1201, 2010 U.S. Dist. LEXIS 32573, at *16-19 (W.D. Pa. Mar. 9, 2010) (“cases which focus on the employee's motive for accessing a computer or his eventual use of the information obtained misunderstand the statute to read ‘exceeds authorized use’ instead of ‘exceeds authorized access’”; “the reach of the CFAA does not extend to instances where the employee was authorized to access the information he later utilized to the possible detriment of his former employer”; recommending grant of motion to dismiss), adopted by, complaint dismissed at 2010 U.S. Dist. LEXIS 31489 (W.D. Pa. Mar. 31, 2010); Clarity Servs. v. Barney, 8:08-cv-2278-T-23TBM, 2010 U.S. Dist. LEXIS 32519, at *13-15, 21-22 (M.D. Fla. Feb. 26, 2010) (adopting narrow definition of authorization and dismissing CFAA claim); American Family Mutual Ins. Co. v. Hollander, 08-CV-1039, 2009 U.S. Dist. LEXIS 16897, at *29-31 (N.D. Iowa Mar. 3, 2009) (where plaintiff insurance company conceded that defendant former insurance agent was authorized to access agency database system (ADS) but nonetheless argued that agent “would have no valid reason for accessing and printing a global list of policyholders,” court concluded plaintiff could not prove that defendant accessed the ADS without authorization or by exceeding his authorized access; reasoning that “[e]ven if the information obtained was subsequently used for an improper purpose, there is no violation of the CFAA”); Bridal Expo, Inc. v. Van Florestein, 4:08-CV-03777, 2009 U.S. Dist. LEXIS 7388, at *33, 37 (S.D. Tex. Feb. 3, 2009) (“declin[ing] to read the CFAA to equate ‘authorization’ with a duty of loyalty to an employer”; granting motion to dismiss CFAA claim); U.S. Bioservices Corporation v. Lugo, 595 F. Supp. 2d 1189, 1194, (D. Kan. 2009) (“the court follows the line of cases that have rejected a reading of the CFAA by which the defendant's intent may determine whether he has acted without authorization or has exceeded his authorized access”; granting motion to dismiss CFAA claims in part); Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929, 934-37 (W.D. Tenn. 2008) (where employee was permitted access to employer's network and any information on that network, court found that “[t]he fact that [the employee] did not have permission to subsequently misuse the data he accessed by sharing it with any of his former employer's competitors is another matter that may be circumscribed by a different statute”; granting motion to dismiss CFAA claim under 18 U.S.C. § 1030 (a)(2)); Condux International, Inc. v. Haugum, 08-4824, 2008 U.S. Dist. LEXIS 100949, at *18-19 (D. Minn. Dec. 15, 2008) (where the “heart of the dispute” was “not the access of the confidential business information but rather the alleged subsequent misuse or misappropriation of that information,” plaintiff failed to state a claim for violations of subsections (a)(2), (a)(4), or (a)(5)(A)(ii) or (iii); granting motion to dismiss); Diamond Power International v. Davidson, 540 F. Supp. 2d 1322, 1342-43 (N.D. Ga. 2007) (finding that a violation of the CFAA “does not depend upon the defendant's unauthorized use of *information*, but rather upon the defendant's unauthorized use of *access*”; emphases in original; dismissing CFAA claim because former employee was authorized to initially access former employer's computers and his level of authorized access included express permission (and password access) to obtain the specific information he later disclosed to competitor); Brett Senior & Associates, P.C. v. Fitzgerald, 06-1412, 2007 U.S. Dist. LEXIS 50833, at *8-9 (E.D. Pa. July 13, 2007) (where former law firm employee converted files to ZIP or PDF format, made a list of clients,

The plain language of the statute, the statute as a whole, its legislative history, and the rule of lenity all support a narrow construction of the CFAA. Specifically, the plain language of subsection 1030(a)(2)(C) and definitional subsection 1030(e)(6) are controlling. See Robinson v. Shell Oil Co., 519 U.S. 337, 340-341, 117 S. Ct. 843, 136 L. Ed. 2d 808 (1997) (instructing courts to interpret a statute based upon its “plain and unambiguous meaning”). Taken together, these CFAA subsections only prohibit improper accessing of computer information; neither subsection makes any reference to accessing information for an unauthorized or improper purpose, or to misuse or misappropriation. See Jet One, 2009 U.S. Dist. LEXIS 72579, at *18; Orbit One, 2010 U.S. Dist. LEXIS 36609, at *27-28 (“reading the phrase[] . . . ‘exceeds authorized access’ to encompass an employee's misuse or misappropriation of information to which the employee freely was given access and which the employee lawfully obtained would depart from the plain meaning of the statute”). Although the term “authorized” is not defined in the statute, courts have construed the term’s ordinary meaning and found that an “an employer gives an employee ‘authorization’ to access a company computer when the employer gives the employee permission to use it.” See Brekka, 581 F.3d at 1132-33 (citing Perrin v. United States, 444 U.S. 37, 42, 100 S. Ct. 311, 62 L. Ed. 2d 199 (1979) (stating that it is a “fundamental canon of statutory construction . . . that, unless otherwise defined, words will be

and copied client information to an external hard drive or CD, court found that “[b]ecause there is no allegation that [employee] lacked authority to view any information in the BSA computer system, the CFAA claim fails”); Lockheed Martin Corp. v. Speed, 6:05-cv-1580-Orl-31KRS, 2006 U.S. Dist. LEXIS 53108, at *15-16 (M.D. Fla. Aug. 1, 2006) (where employees were permitted to access company computer and “to access the precise information at issue, the Employees did not exceed authorized access”; granting motion to dismiss CFAA claim under 18 U.S.C. § 1030(a)(4)); SecureInfo Corp. v. Telos Corp., 387 F. Supp. 2d 593, 598, 608-10 (E.D. Va. 2005) (granting motion to dismiss CFAA claims because defendants were granted access to server and information on the server; consequently, they were “entitled to obtain” information on the server and plaintiff failed to properly allege that defendants had “unauthorized access” to the server or accessed the server in “excess of authority” within the meaning of the statute)

interpreted as taking their ordinary, contemporary, common meaning.”)); Gast, 535 F. Supp. 2d at 965 (finding that authorization is commonly understood as “[t]he act of conferring authority; permission” and concluding that “[s]ection 1030(e)(6) contemplates that an “exceeds authorized access” violation occurs where the defendant first has *initial* “authorization” to access the computer”; emphasis added; other citations omitted). In other words, if an employer gives an employee a password to initially access a computer, the employee has authorized access to the computer and that authorization is only limited to whatever information is available through such password access.

The statute as a whole confirms that Congress’s intent was not to prohibit an employee’s access for an improper purpose or improper use of access. Such broad violations are not compensable, because the statute’s damages definitions require any compensation sought to be the result of computer impairment or computer damage. See 18 U.S.C. §§ 1030(e)(8), (11); Jet One, 2009 U.S. Dist. LEXIS 72579, at *19 (“These narrow definitions are wholly consistent with a limited Congressional intent in passing the CFAA - prohibiting people from ‘hacking’ into someone else’s computer system, an act which can corrupt ‘the integrity or availability of data, a program, a system, or information’ or lead to ‘interruption of service.’”; “it confounds common sense to suggest that Congress created a private right of action for, essentially, misappropriating confidential information, but expressly denied prospective plaintiffs any relief for this kind of ‘violation.’”); Orbit One, 2010 U.S. Dist. LEXIS 36609, at *29 (same). Moreover, both the Jet One and Orbit One courts found that the Second Circuit’s affirmance of a decision denying CFAA claimants a remedy for competitive harm suffered as a result of misuse or misappropriation, constituted an implicit adoption of a narrow statutory construction. See Jet One, 2009 U.S. Dist. LEXIS 72579, at *19-20 (citing Nexans Wires S.A. v. Sark-USA, Inc.,

166 Fed. Appx. 559, 562-563 (2d Cir. 2006));⁵ Orbit One, 2010 U.S. Dist. LEXIS 36609, at *29-30.

In addition, “the legislative history confirms that the CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information.” Gast, 535 F. Supp. 2d at 966 (analyzing Senate reports). Indeed, Congress’s statutory amendments repudiated any prohibition of misuse:

[I]n 1986 Congress amended the CFAA to substitute the phrase “exceeds authorized access” for the phrase “or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend.” By enacting this amendment, and providing an express definition for “exceeds authorized access,” the intent was to “eliminate coverage for authorized access that aims at ‘purposes to which such authorization does not extend,’” thereby “removing from the sweep of the statute one of the murkier grounds of liability, under which a [person’s] access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization.”

Werner-Matsuda, F. Supp. 2d at 499 n. 12 (emphasis added) (citations to Senate reports omitted).

Finally, the rule of lenity should guide the Court's interpretation of the CFAA because its construction of subsection 1030(a)(2)(C) applies equally in criminal and civil contexts. See Leocal v. Ashcroft, 543 U.S. 1, 11 n.8, 125 S. Ct. 377, 160 L. Ed. 2d 271 (2004) (holding that where a statute “has both criminal and noncriminal applications,” courts should interpret the statute consistently). The rule of lenity “ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered.” Orbit One, 2010 U.S. Dist. LEXIS 36609, at *21. Applying that rule, courts have found that that common law misappropriation, a breach of contract, and a breach of an employee’s duty of loyalty that

⁵ The Nexans case is discussed more fully in Point I.B below.

involve a computer should not be swept it into the CFAA's ambit of criminal liability. Jet One, 2009 U.S. Dist. LEXIS 72579, at *21 (refusing to "transform what has always been a common law civil tort (i.e., misappropriation of confidential information) into a federal criminal offense"); Orbit One, 2010 U.S. Dist. LEXIS 36609, at *30 (same); Brekka, 581 F.3d at 1135 (finding that employee would not have fair warning of possible criminal violation arising from breach of fiduciary duty to employer "[i]f the employer has not rescinded the defendant's right to use the computer"); Gast, 535 F. Supp. 2d at 967 (statutory text does not support criminalizing computer-based breaches of contract) (citing Whitman v. American Trucking Associations, 531 U. S. 457, 468, 121 S. Ct. 903, 149 L. Ed. 2d 1 (2001) (Congress does not "hide elephants in mouseholes"))).

Here, Plaintiff's Complaint fatally alleges that "the Former Employee Defendants each had authority to access Aon's protected computers[.]" See FAC, ¶ 66. Plaintiff also concedes that it granted "password protect[ed] computer access to only Aon employees." See FAC, ¶ 22. Nowhere in Plaintiff's Complaint, however, is there any allegation that the individual defendants' password access was ever rescinded or that they exceeded such access by obtaining information that their passwords did not entitle them to obtain. See Orbit One, 2010 U.S. Dist. LEXIS 36609, at *30-31 (finding that former executives did not exceed authorized access because they "they concededly were granted unfettered access to [counterclaimant's] computer system and information residing on it"). Rather, Plaintiff apparently alleges that the individual defendants exceeded authorized access by obtaining information "for the purpose of facilitating an unlawful solicitation of business or employees for the benefit of themselves or of an Aon competitor and to the detriment of Aon" and that such access was excessive because it

was inconsistent with Aon's policies and Kornblau and Angoff's agreements with Aon. See FAC, ¶¶ 28, 33, 36, 67.

For the purposes of imposing civil and/or criminal liability under CFAA, Plaintiff cannot plausibly contend that the individual defendants' authorization is an on / off switch that is triggered whenever Aon objects to their computer activities after the conduct has already occurred. Nothing in the statute warrants recognition of a claim premised on an employer's unilateral authority to define authorization. Such authority could be wielded arbitrarily against an unwitting computer user who did not – and, indeed, could not – know the boundaries of his or her authorized access. Because of this self-evident danger, courts have declined to adopt a broad statutory construction even when the computer user should have known that he or she was acting against his employer's interest. See Jet One, 2009 U.S. Dist. LEXIS 72579, at *16 (allegations that defendant employee was recruited and paid to take plaintiff's computer records, including client list, for corporate defendant's benefit insufficient); Orbit One, 2010 U.S. Dist. LEXIS 36609, at *30-*31 (dismissing CFAA claim asserting that individuals took electronic proprietary information prior to leaving company for the purpose of competing with it); Brekka, 581 F.3d at 1130, 1134-35 (rejecting CFAA claim based on former employee's emailing of documents, including lists of plaintiff's former and current patients, to himself and to his wife to advance his own competing business). Allowing such a claim would effectively rewrite the statute to permit federal civil actions – as well as criminal charges – for what may amount to nothing more than garden-variety misappropriation and breach of contract. The Court should reject Aon's attempt to federalize and criminalize such state law claims, limit CFAA to “prohibiting people from ‘hacking’ into someone else's computer system,” and hold that Plaintiff has failed to establish

that the individual defendants exceeded their password access to Aon's computers. See Jet One, 2009 U.S. Dist. LEXIS 72579 at *19.

B. Plaintiff Cannot Establish An Actionable "Loss."

The CFAA generally permits a civil action if the plaintiff "suffers damage or loss by reason of a violation of this section," but only if the plaintiff can satisfy one of five factors. 18 U.S.C. § 1030(g). The only applicable factor here requires Plaintiff to establish a "loss to 1 or more persons during any 1-year period . . . aggregating at least \$ 5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I). The term "loss" is defined as a "reasonable cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service[.]" 18 U.S.C. § 1030(e)(11) (emphases added). The term "damage" is defined as "impairment to the integrity of availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8).

In Nexans Wires S.A. v. Sark-USA, Inc., Judge Cederbaum thoroughly reviewed the CFAA's legislative history and found that "the meaning of 'loss' . . . has consistently meant a cost of investigating or remedying damage to a computer, or a cost incurred because the computer's service was interrupted." 319 F. Supp. 2d 468, 475 (S.D.N.Y. 2004) (emphasis added) (converting motion to dismiss into motion for summary judgment and dismissing CFAA claim), aff'd, 166 Fed. Appx. 559, 562-563 (2d Cir. 2006). Further, she found that under the plain language of the statute, any alleged lost revenue must be lost "because of [an] interruption of service." 319 F. Supp. 2d at 477 (emphasis added). She thus held that revenue lost merely "because the information was used by the defendant to unfairly compete after extraction from a computer does not appear to be the type of "loss" contemplated by the statute." Id. at 478;

accord B.U.S.A. Corp. v. Ecogloves, Inc., 05 Civ. 9988 (JSR), 2009 U.S. Dist. LEXIS 89035 at *26 (S.D.N.Y. Sept. 26, 2009) (dismissing CFAA claim because plaintiffs failed to show that former employee “caused an ‘interruption of service’ -- at most, plaintiffs were unable to access some of her past emails for an unspecified period of time”); Civic Ctr. Motors, Ltd. v. Mason St. Imp. Cars, Ltd., 387 F. Supp. 2d 378, 382 (S.D.N.Y. 2005) (finding compensation sought “for lost profits resulting from Defendant's unfair competitive edge and for their now wasted investment in the development and compilation of the database information” were not “the result of computer impairment or computer damage” and, therefore, are not “compensable ‘losses’ under the CFAA”; granting motion to dismiss and denying motion for preliminary injunction).

Here, Plaintiff inadequately and, in conclusory fashion, alleges a loss “well in excess of \$5,000” comprised of: (1) “the costs of investigating defendants’ actions”; (2) “assessing the resulting damages, restoring the data and information altered and/or deleted by the Former Employee Defendants”; and (3) “the costs associated with the interruption to Aon’s business, and damages and/or losses in loss of revenue and business interruption to Aon.” FAC, ¶ 69. With respect to the first asserted loss, Plaintiff’s claim fails because it alleges costs incurred in investigating the individual defendants’ actions, but without alleging any connection to computer damage or impairment. See Nexans Wires S.A., 319 F. Supp. 2d at 475. The third asserted loss clearly relates to Plaintiff’s allegation that the individual defendants obtained information “for the purpose of facilitating an unlawful solicitation of business or employees for the benefit of themselves or of an Aon competitor and to the detriment of Aon.” FAC, ¶ 67. Because Plaintiff alleges only misappropriation resulting in lost *business* instead of alleging a loss resulting from interruption of computer service, Plaintiff’s allegations are insufficient as a matter of law. See Jet One, 2009 U.S. Dist. LEXIS 72579 at *22 (granting motion to dismiss

CFAA claim because plaintiff merely alleged that defendants “obtained ‘confidential and proprietary information’ and used such information to Plaintiff’s detriment - while not connecting this detriment to any ‘impairment’ to its computer system, ‘damage assessment,’ data restoration expense, or ‘interruption of service’”).

With respect to the second asserted loss, Plaintiff only alleges that Angoff and Wendleken accessed files while they were still employed by Aon. See FAC, ¶¶ 57-59, 61. Plaintiff fails to specifically allege that Angoff or Wendleken obtained information and thereby caused damage to or interrupted the service of any of Aon’s computers. See 18 U.S.C. § 1030(g) (civil action may be brought “against the violator” if plaintiff suffers statutorily defined damage “by reason of a violation of this section”). Plaintiff also alleges that Kornblau downloaded and deleted certain files. See FAC, ¶¶ 52, 53. However, mere downloading or copying of files does not constitute “damage.” See Condux Int’l, Inc. v. Haugum, 08-4824, 2008 U.S. Dist. LEXIS 100949, at *20-25 (D. Minn. Dec. 15, 2008) (holding that “the complained of activity must have an effect on the binary coding used to create, store, and access computerized representations of information”) (collecting cases). Moreover, Plaintiff does not allege that Kornblau’s alleged actions resulted in the “*permanent* deletion or removal” of any files. See Lockheed Martin Corp. v. Speed, 6:05-cv-1580-Orl-31KRS, 2006 U.S. Dist. LEXIS 53108, at *26-27 (M.D. Fla. Aug. 1, 2006) (emphasis added). It is both implausible and unreasonable to infer that Plaintiff suffered an actionable loss when courts have recognized that “merely pressing the delete key on a computer *does not remove data* but rather ‘removes the index entry and pointers to the data file so that the file appears no longer to be there’” and that such files “are easily recoverable.” Dedalus Foundation v. Banach, 09 Civ. 2842 (LAP), 2009 U.S. Dist. LEXIS 98606, at *11 (S.D.N.Y. Oct. 15, 2009) (emphasis added) (quoting International Airport Ctrs., L.L.C. v. Citrin,


440 F.3d. 418, 419 (7th Cir. 2006)). Accordingly, the Court should dismiss Plaintiff's CFAA claim because Plaintiff fails to allege any damage to a computer or interruption of service.

CONCLUSION

For the foregoing reasons, Defendants respectfully request that the Court dismiss Plaintiff's First Amended Complaint in its entirety, with prejudice, and grant such other and further relief as the Court deems just and proper.

Respectfully submitted,

JACKSON LEWIS LLP
59 Maiden Lane
New York, New York 10038-4502
(212) 545-4000

By: 
Clifford R. Atlas (CA 9512)
Marjorie Kaye, Jr. (MK 7141)
Ravindra K. Shaw (RS 1944)

ATTORNEYS FOR DEFENDANTS

Dated: May 27, 2010
New York, New York