[*1]

Spec Simple, Inc. v Designer Pages Online LLC
2017 NY Slip Op 27159
Decided on May 10, 2017
Supreme Court, New York County
Kornreich, J.
Published by New York State Law Reporting Bureau pursuant to Judiciary Law § 431.
This opinion is uncorrected and subject to revision before publication in the printed Official Reports.

Decided on May 10, 2017

Supreme Court, New York County

Spec Simple, Inc., Plaintiff,

against

Designer Pages Online LLC and FXFOWLE Architects LLP, Defendants.

651860/2015

Peter Brown & Associates PLLC, for plaintiff

The Adams Law Firm LLC, for DPO

Satterlee Stephens LLP, for FXFOWLE

Shirley Werner Kornreich, J.

Motion sequence numbers 001 and 002 are consolidated for disposition.

Defendants Designer Pages Online LLC (DPO) and FXFOWLE Architects, LLP (FXFOWLE) separately move,[FN1] pursuant to CPLR 3211, to dismiss the amended complaint (the AC). Plaintiff Spec Simple, Inc. (plaintiff or Spec Simple) opposes the motions. Defendants' motions are granted in part and denied in part for the reasons that follow.

I. Factual Background & Procedural History

As this is a motion to dismiss, the facts recited are taken from the AC (*see* Dkt. 11)[FN2] and the documentary evidence submitted by the parties.

Plaintiff, founded in 1992, operates databases used by "the architectural, interior design, engineering, facility management and furniture professions." AC ¶ 1. It alleges:[FN3]

> In the period before widespread Internet access, most professional design firms invested in large and expensive libraries of catalogues and reference material to support their design professionals. The largest firms maintained costly staffs and librarians devoted to keeping this rapidly changing volume of information current. Searching for specific [*2]classes of information was often laborious and time-consuming. The innovative Internet-accessible website and database systems and services created by Spec Simple were designed to utilize the unique database search capabilities of computers to locate comprehensive listings of products for design professionals rapidly, and with the minimum of effort. The features of the Spec Simple system are uniquely designed to access and organize the information relating to the products offered for sale to the architectural, interior design, engineering and facilities management industries from around the world. The product information has been collected and organized for 23,000 companies located in the United States, and approximately forty other countries.

In the two decades since its founding, Spec Simple's efforts have been directed to developing the unique and proprietary structure, sequence and organization for its user interface, website and database systems and services, including its functions and features, and for the organization of the information provided to its customers Spec Simple's password-protected databases, which it calls virtual libraries, consist of information gathered from third parties (primarily product vendors and dealers) (collectively the "Virtual Library") through expenditure of significant time and expense over the past twenty years. Spec Simple has organized the information in its Virtual Library to make it easily searchable and user friendly through a variety of innovative features. The Virtual Library is available for the exclusive use of authorized users who must subscribe to the Spec Simple service.

Spec Simple routinely implements security procedures to protect its proprietary information from misuse by employees and third parties. Internally, employee access is limited by passwords and restrictions relating to employee functions. For third parties, access to the Virtual Library is restricted to subscribers of Spec Simple's services who have entered into written subscription agreements. Generally, Spec Simple's subscribers pay a monthly usage fee and a monthly maintenance fee. Each individual user employed by a subscriber is given a unique password.

Subscribers to Spec Simple's services are given the opportunity to customize the system's functions, features and Virtual Library data accessible by the subscriber's employees based on the type of work performed by the customer. This customization creates efficiency for the users and fosters customer loyalty to the subscriber business. A competitor with access to these custom features and insights into the customer's requirements would have the ability to undermine Spec Simple's business relationship with its subscribers. The Virtual Library is one of Plaintiff's primary and most valuable assets and it is a significant part of Spec Simple's competitive advantage in the marketplace.

In addition, Spec Simple maintains a staff of information specialists who have responded to the unique needs and specific inquiries of its subscribers and users for over twenty years, through features such as the "Ask the Librarian" feature. These unique questions and answers provide solutions to a broad array of designer issues. This singular collection of user inquires reflects the specific concerns and problems facing design professionals. Spec Simple has curated this collection of original, proprietary information and has made it a key feature of the Spec Simple site.

To further support its subscribers and users, Spec Simple offers a private communication service. (the "Spec Simple Email System"). The Spec Simple Email System allows users [*3]to directly communicate via email with vendors listed in the Virtual Library to obtain confidential price quotes, product specifications, private meetings

> with vendors and vendor literature and materials. The same Spec Simple Email System permits private communications among users in the same subscriber firm, particularly to obtain vendor ratings or recommendations. These company-wide notes assist a company in maintaining quality and design standards in its work. As part of the "Ask a Librarian" service, users can also employ the Spec Simple Email System to submit confidential inquiries to Spec Simple's data "librarians," who assist users conducting more complex searches. All of the above communications are stored on Spec Simple's web servers as part of the Spec Simple Email System.
>
> In its current iteration, the Spec Simple website offers certain basic information, with no customer support, in the "free" portion of the website available to the public via the Internet. Subscribers to the Spec Simple service obtain access to the Virtual Library in a fashion similar to lawyers using the WestLaw or LexisNexis service. Each unique user is provided access to the site via a custom password which is confidential to that individual. Users are instructed not to share the password or give unauthorized parties access to the Spec Simple site.

AC ¶¶ 18-29 (paragraph numbering and some breaks omitted).

DPO is a company that competes with plaintiff (i.e., like Westlaw competes with Lexis). FXFOWLE is an architectural firm. FXFOWLE is a former client of plaintiff. It is a current client of, and has an ownership interest in, DPO. In this action, plaintiff claims that while FXFOWLE was its client, in violation of the parties' contract and two federal statutes, FXFOWLE illicitly provided plaintiff's proprietary information in plaintiff's database to DPO (which, as noted, FXFOWLE has an ownership interest in) to facilitate unfair competition.

FXFOWLE began using plaintiff's services in 2009. On August 14, 2014, plaintiff's founder, Suzanne Swift, noticed while reviewing a usage report that Lauren Zailyk, an employee of FXFOWLE, conducted approximant 1,000 searches in plaintiff's system on that day. Swift found this to be highly unusual for a single user on a single day. "On closer examination of the logs, including the Internet protocol ("IP") addresses of the accessing computers, Ms. Swift quickly determined that the 1000 queries came from multiple computers located around the world." AC ¶ 39. The next day, on August 15, 2014, Erica Godun, another FXFOWLE employee, admitted to Swift that she had given "Zailyk's Spec Simple username and password to Jake Slevin, [DPO's] Chief Executive Officer, so that he 'could take a look around.'" AC ¶ 40. Plaintiff alleges that "[a]s a result of the 1000 searches, [DPO] downloaded for its own benefit large portions of Spec Simple's Virtual Library

and/or information or emails stored in Spec Simple's Email System." AC ¶ 42. Plaintiff further alleges that DPO used this information to "lure away Spec Simple's clients." AC ¶ 43.

Plaintiff commenced this action by filing its original complaint on May 28, 2015, and filed the AC on June 29, 2016. Plaintiff asserts seven causes of action, numbered here as in the AC: (1) violation of the Computer Fraud and Abuse Act (the CFAA), 18 USC § 1030, asserted against both defendants; (2) violation of the Stored Communications Act (the SCA), 18 USC § [*4]2701, asserted against both defendants;[FN4] (3) breach of contract (an October 1, 2013 agreement), asserted against FXFOWLE; (4) breach of contract (the terms of service of plaintiff's website), asserted against both defendants; (5) misappropriation of confidential information, asserted against both defendants; (6) unjust enrichment, asserted against DPO; and (7) violation of General Business Law (GBL) § 349 (unfair and deceptive trade practices), asserted against DPO. Defendants filed the instant motions to dismiss the AC on September 29, 2016. Defendants seek dismissal of all claims except the breach of contract claims.[FN5] The court reserved on the motions after oral argument. *See* Dkt. 31 (2/22/17 Tr.).

II. Discussion

A. Legal Standard

On a motion to dismiss, the court must accept as true the facts alleged in the complaint as well as all reasonable inferences that may be gleaned from those facts. *Amaro v Gani Realty Corp.*, 60 AD3d 491 (1st Dept 2009); *Skillgames, LLC v Brody*, 1 AD3d 247, 250 (1st Dept 2003), citing *McGill v Parker*, 179 AD2d 98, 105 (1st Dept 1992); *see also Cron v Hargro Fabrics, Inc.*, 91 NY2d 362, 366 (1998). The court is not permitted to assess the merits of the complaint or any of its factual allegations, but may only determine if, assuming the truth of the facts alleged and the inferences that can be drawn from them, the complaint states the elements of a legally cognizable cause of action. *Skillgames*, *id.*, citing *Guggenheimer v Ginzburg*, 43 NY2d 268, 275 (1977). Deficiencies in the complaint may be remedied by affidavits submitted by the plaintiff. *Amaro*, 60 NY3d at 491. "However, factual allegations that do not state a viable cause of action, that consist of bare legal conclusions, or that are inherently incredible or clearly contradicted by documentary evidence are not entitled to such consideration." *Skillgames*, 1 AD3d at 250, citing *Caniglia v Chicago Tribune-New York News Syndicate*, 204 AD2d 233

(1st Dept 1994). Further, where the defendant seeks to dismiss the complaint based upon documentary evidence, the motion will succeed if "the documentary evidence utterly refutes plaintiff's factual allegations, conclusively establishing a defense as a matter of law." *Goshen v Mutual Life Ins. Co. of NY*, 98 NY2d 314, 326 (2002) (citation omitted); *Leon v Martinez*, 84 NY2d 83, 88 (1994).

B. CFAA

"The CFAA criminalizes, *inter alia*, 'intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] ... information from any protected computer,' 18 U.S.C. § 1030(a)(2)(C), and 'intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss,' *id.* § 1030(a)(5)(C)." *Sewell v Bernardin*, 795 F3d 337, 339-40 (2d Cir 2015). In other words, the CFAA "provides two ways of committing the crime of improperly accessing a protected computer: (1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly." *Facebook, Inc. v Power Ventures, Inc.*, 844 F3d 1058, 1066 (9th Cir 2016), quoting *Musacchio v United States*, 136 SCt 709, 713 (2016) (noting that § [*5]1030(e)(6) defines "exceeds authorized access" as accessing "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.") The CFAA "also provides a civil cause of action to '[a]ny person who suffers damage or loss by reason of a violation of this section.'" *Sewell*, 795 F3d at 340, quoting § 1030(g).

While the CFAA is the subject of contentious litigation over its meaning, particularly with respect to the meaning of "exceeds authorized access",[FN6] there is federal authority suggesting that while merely violating a website's terms of service is not a violation of the CFAA (at least not a criminal violation), illicitly accessing a competitor's website to facilitate unfair competition may indeed be a CFAA violation. In *Facebook*, the Ninth Circuit explained:

> In [*United States v Nosal*, 676 F3d 854 (9th Cir 2012) (en banc) ("*Nosal I*")], a criminal case, we considered whether a group of employees who logged on to a work computer, downloaded information from a confidential database, and transferred it to a competing business "exceed[ed] authorized access." *Id.* at 856. Wary of creating a sweeping Internet-policy mandate, we applied the rule of lenity to the CFAA and reversed liability for the

> defendant. *Id.* at 863. The decision broadly described the application of the CFAA to the websites' terms of service. "Not only are the terms of service vague and generally unknown ... but website owners retain the right to change the terms at any time and without notice." *Id.* at 862. As a result, imposing criminal liability for violations of the terms of use of a website could criminalize many daily activities. Accordingly, "the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions. If Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly." *Id.* at 863.

Facebook, 844 F3d at 1066-67.

> The Ninth Circuit then explained its "two general rules in analyzing authorization under the CFAA":
>
> First, a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly. Once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability. Second, **a violation of the terms of use of a website—without more—cannot establish liability under the CFAA**.

Facebook, 844 F3d at 1067 (emphasis added). The court then stated that its analysis was consistent with its decision in *United States v Nosal*, 844 F3d 1024, 1030 (9th Cir 2016) (*Nosal II*).[FN7] The *Nosal II* court explained that "[a]lthough the meaning of 'exceeds authorized access' in the CFAA has been subject to much debate among the federal courts, the definition of 'without authorization' has not engendered dispute." *Id.* at 1036; *see id.* n.11 (collecting cases). The court then explained that there was no authority supporting the proposition "that a former [*6]employee whose computer access has been revoked can access his former employer's computer system and be deemed to act with authorization." *Id.* at 1036-37. The court then suggested that unauthorized access accomplished for the purpose of engaging in unfair competition is a violation of the CFAA. *See id.* at 1037. Rejecting the approach advocated by the dissent, the majority wrote:

> In the face of multiple circuits that agree with our plain meaning construction of the statute, the dissent would have us ignore common sense and turn the statute inside out. Indeed, the dissent frames the question upside down in assuming that permission from FH is at issue. **Under this approach, ignoring reality and practice, an employee could undermine the company's ability to control access to its own computers by willy nilly giving out passwords to anyone outside the company—former employees whose access had been revoked,**

> **competitors, industrious hackers or bank robbers who find it less risky and more convenient to access accounts via the Internet rather than through armed robbery**.

Nosal II, 844 F3d at 1037 (emphasis added). The *Nosal II* court viewed this as a form of fraud, not merely a terms of service violation. *See id.* at 138.

Plaintiff relies on *Nosal II*. It alleges that FXFOWLE gave the CEO of DPO, plaintiffs' direct competitor, access to plaintiff's database, which plaintiff claims DPO used to improve its own product and lure away customers. According to plaintiff, this is the very sort of fraud that *Nosal II* suggests is sufficient to state a claim under the CFAA. However, plaintiff has missed the distinction, noted in *Nosal II*, between accessing a computer without any authorization (as DPO did) and exceeding the scope of permitted access (FXFOWLE's employees providing access to DPO). Yet, even if FXFOWLE's exceeding the scope of its permitted access is not a CFAA violation, there is a strong case to be made that DPO's employees, who had no reasonable basis to believe that DPO's access was authorized, may still be held liable under the CFAA.

Under the facts alleged in the AC, the truth of which must be assumed for the purposes of this motion to dismiss, it is reasonable to infer that defendants' alleged unauthorized access was made with the requisite scienter. A plausible inference of ill intent may be drawn from a customer's single login being used to conduct 1,000 searches on a single day from computers around the world. That these searches were made by a competitor in breach of FXFOWLE's contract with plaintiff permits an additional inference that such access was for the purpose of unfair competition.

This is not a case where an authorized user merely improperly accessed plaintiff's information. Rather, the wrong here was that an authorized user (FXFOWLE) allegedly gave an unauthorized user (DPO) credentials so DPO, a competitor of which FXFOWLE is a part owner, could access plaintiff's information to enable DPO's alleged theft of plaintiff's proprietary database structure. DPO could not have reasonably believed that it had the right (or plaintiff's consent) to access plaintiff's database. Even if all it did was innocuously peruse, but not copy or utilize anything, DPO has no legitimate basis to contend that it had plaintiff's consent to do so. The surreptitious manner in which it allegedly accessed the database belies such an inference. Nor is this a situation of a faithless employee who simply exceeded the scope of his permitted access.

That being said, as noted earlier, this is an area of law in which there is much disagreement. *See, e.g., LivePerson, Inc. v 24/7 Customer, Inc.*, 83 FSupp3d 501, 512 (SDNY 2015) (Sweet, J.) (collecting district court cases in the Second Circuit reflecting disagreement on [*7]interpretation of the CFAA); *see also United States v Yücel*, 97 FSupp3d 413, 422 (SDNY 2015).[FN8] This court need not reach the unsettled issues raised by the parties because plaintiff has failed to plead damages recoverable within the meaning of the statute.[FN9] Causing a "loss" in excess of $5,000 [*see LivePerson,* 83 FSupp3d at 511] is the requisite third element of a CFAA claim. The losses set forth in the AC — unfair competition losses due to DPO's poaching customers after upgrading its product with the benefit of plaintiff's misappropriated trade secrets — are not recoverable under the CFAA.

Loss is defined in § 1030(e)(11) to mean "any reasonable cost to any victim, including the 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." "Damages" is defined in § 1030(e)(8) as "any impairment to the integrity or availability of data, a program, a system, or information." Based on these definitions, courts in the Second Circuit have consistently held that the damages recoverable on a CFAA claim are (absent an allegation of interruption of service, which is not alleged) limited to recovery for harm to the computer system that was accessed without authorization.[FN10] Damages for unfair competition injuries, such as those pleaded by plaintiff in this case, are not recoverable under the CFAA. *See Reis, Inc. v Lennar Corp.*, 2016 WL 3702736, at *5 (SDNY 2016) (collecting cases); *Orbit One Commc'ns, Inc. v Numerex Corp.*, 692 FSupp2d 373, 386 (SDNY 2010) (noting the Second Circuit "denies CFAA claimants a remedy for competitive harm suffered as a result of misuse or misappropriation."), citing *Nexans Wires S.A. v Sark-USA, Inc.*, 166 FApp'x 559, 562 (2d Cir 2006); *see also Jet One Group, Inc. v Halcyon Jet Holdings, Inc.*, 2009 WL 2524864, at *6 (EDNY 2009) (noting that in *Nexans*, "the Second Circuit affirmed a well-reasoned decision by [Judge] Cederbaum recognizing that—at least with respect to damages—the CFAA says exactly what it means. Specifically, the Second Circuit held that a plaintiff cannot recover 'lost revenue' under the CFAA unless that lost revenue derives from an 'interruption of service.' In so doing, the Second Circuit affirmed Judge

Cederbaum's holding that **a plaintiff cannot recover revenue lost 'as a result of defendants' ability to unfairly compete for business' due to the misappropriated proprietary information**.") (citations omitted; emphasis added).[FN11]

This court will follow the consensus among Southern District judges and the Second Circuit's decision in *Nexans* (albeit in a non-precedential summary order), which hold that recovery of unfair competition damages under the CFAA is not permitted. *See Obeid v Mack*, 2017 WL 1215753, at *8 (SDNY 2017) ("Any recoverable damage or loss under the CFAA must be directly caused by computer impairment or damage."); *Mount v PulsePoint, Inc.*, 2016 WL 5080131, at *8 (SDNY 2016), *aff'd on other grounds*, 2017 WL 1147191 (2d Cir Mar. 27, 2017); *Garland-Sash v Lewis*, 2011 WL 6188712, at *3-4 (SDNY 2011); *Marketing Tech. Solutions, Inc. v Medizine LLC*, 2010 WL 2034404, at *7 (SDNY 2010). Indeed, a similar consensus appears to be developing outside of the Second Circuit. *See Brown Jordan Int'l, Inc. v Carmicle*, 846 F3d 1167, 1174 (11th Cir 2017); *BHRAC, LLC v Regency Car Rentals, LLC*, 2015 WL 3561671, at *3 (CD Cal 2015) ("The only injury Plaintiff alleges as a result of the theft the Information is the loss of business from Regency poaching its customers. As other courts have observed, that is not the sort of injury for which the CFAA provides a remedy."). Since unfair competition damages are the only damages pleaded, plaintiff's CFAA claim is dismissed.

C. SCA

The SCA, 18 USC § 2701(a), prohibits accessing another person's emails without authorization. *Sood v Rampersaud*, 2013 WL 1681261, at *2 (SDNY 2013); *see* § 2701(c) (absolving party from liability if person whose emails were accessed provided authorization). In this case, plaintiff alleges that DPO employees accessed some (no specificity is provided) of the emails FXFOWLE stored in plaintiff's email system. But it was FXFOWLE's own employees that provided such access to DPO. Plaintiff has no standing to complain about someone accessing emails that are not its own communications. Such a claim belongs to the owner of the email account whose privacy the SCA is meant to protect.[FN12] Thus, even if the AC might be fairly read to allege that the access provided by FXFOWLE to DPO did not include the right to view FXFOWLE's emails (because it allegedly was Godun who provided Zailyk's login to Slevin), plaintiff lacks standing to sue under the SCA because plaintiff suffered no harm from the alleged SCA violation.

D. Misappropriation of Confidential Information & Unjust Enrichment

"[A] trade secret [is] any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over [*8]competitors who do not know or use it." *Ashland Mgmt. Inc. v Janien*, 82 NY2d 395, 407 (1993) (quotation marks omitted). The First Department has held that a database that meets the criteria set forth in *Ashland* may qualify for trade secret protection. *Invesco Institutional (N.A.), Inc. v Deutsche Inv. Mgmt. Americas, Inc.*, 74 AD3d 696, 697 (1st Dept 2010) ("the court properly found that plaintiff had a protectable trade secret in the proprietary nature of its software and database structure."); *see Schroeder v Pinterest Inc.*, 133 AD3d 12, 27 (1st Dept 2015) ("In determining whether information constitutes a trade secret, 'several factors should be considered: (1) the extent to which the information is known outside of [the] business; (2) the extent to which it is known by employees and others involved in [the] business; (3) the extent of measures taken by [the business] to guard the secrecy of the information; (4) the value of the information to [the business] and [its] competitors; (5) the amount of effort or money expended by [the business] in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.'"), quoting *Ashland*, 82 NY2d at 407.

On this motion, defendants do not argue that no aspect of plaintiff's database is a protectable trade secret. Rather, defendants contend that plaintiff's claim for misappropriation of confidential information should be dismissed for failure to *plead* sufficient detail about its trade secrets. The specificity demanded by defendants must be provided in discovery, but need not be pleaded. The very case on which defendants rely, *MSCI Inc. v Jacob*, 120 AD3d 1072 (1st Dept 2014), was a decision requiring trade secret specificity to be provided in discovery, not in the complaint. *See id.* at 1075-76 (addressing trade secret source code to be produced in discovery).[FN13] Moreover, a reasonable inference can easily be drawn from the well pleaded allegations in the AC as to the nature of the trade secrets contained in plaintiff's database, which, if publicly disclosed, would compromise their secret nature. Defendants' motions to dismiss plaintiff's claim for misappropriation of trade secrets, therefore, is denied.

With respect to plaintiff's unjust enrichment claim, DPO (the only defendant the claim is asserted against) does not proffer any argument in support of dismissal other than failure to plead trade secrets with sufficient particularity, an argument

rejected above. The unjust enrichment claim, therefore, is not dismissed.

E. GBL § 349.

It is well settled that a claim under GBL § 349 cannot be maintained absent an allegation of "consumer oriented" deceptive conduct. *Koch v Acker, Merrall & Condit Co.*, 18 NY3d 940, 941 (2012); *see Scarola v Verizon Commc'ns, Inc.*, 146 AD3d 692, 693 (1st Dept 2017) (the challenged conduct was not consumer-oriented. The account was a business, not a consumer, account. Nor did defendant's conduct have 'a broader impact on consumers at large.'"), quoting *Oswego Laborers' Local 214 Pension Fund v Marine Midland Bank, N.A.*, 85 NY2d 20, 25 (1995).[FN14] This claim is dismissed because plaintiff is not a consumer. This is a dispute between [*9]competing businesses. *See Camacho v IO Practiceware, Inc.*, 136 AD3d 415, 416 (1st Dept 2016) ("this is essentially a private contract dispute relating to the specific facts at hand."). Accordingly, it is

ORDERED that defendants' motions to dismiss are granted to the extent of dismissing the first, second, and seventh causes of action and denied as to the fifth and sixth causes of action; and it is further

ORDERED that the parties are to appear in Part 54, Supreme Court, New York County, 60 Centre Street, Room 228, New York, NY, for a preliminary conference on June 20, 2017, at 11:30 in the forenoon, and the parties' pre-conference joint letter shall be e-filed and faxed to Chambers at least one week beforehand.

Dated: May 10, 2017

Hon. Shirley Werner Kornreich
J.S.C.

Footnotes

Footnote 1: Defendants filed separate motions (and are represented by separate counsel), but moved on essentially identical grounds and have joined in the arguments made in each other's briefs.

Footnote 2: References to "Dkt." followed by a number refer to documents filed in this action on the New York State Courts Electronic Filing system (NYSCEF).

Footnote 3: The extensive block quoting from the AC is provided to demonstrate the detailed nature of plaintiff's trade secret allegations, which are relevant to refute defendants' contention (rejected herein) that plaintiff failed to sufficiently plead a claim for misappropriation of trade secrets.

Footnote 4: It is nonsensical for plaintiff to plead an SCA claim against FXFOWLE because, as explained herein, the claim is based on DPO improperly accessing *FXFOWLE's emails*.

Footnote 5: While the contract claims are not the subject of these motions to dismiss, it is worth noting that the October 1, 2013 contract between plaintiff and FXFOWLE expressly prohibits FXFOWLE from disclosing plaintiff's confidential information. *See* Dkt. 30 at 5.

Footnote 6:*See generally* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143 (2016).

Footnote 7: The opinion originally known as *Nosal II*, 828 F3d 865, was issued on July 5, 2016 and was superseded by an amended opinion issued on December 8, 2016, 844 F3d 1024. The parties' briefs only cite to the now superseded opinion in *Nosal II*. They failed to appraise the court of the updated opinion, which was issued by the Ninth Circuit between the time the briefing was completed (October 24, 2016) and oral argument (February 22, 2017).

Footnote 8:*See also* Audra A. Dial & John M. Moye, Kilpatrick Townsend & Stockton LLP, *The Computer Fraud and Abuse Act and Disloyal Employees: How Far Should the Statute Go to Protect Employers from Trade Secret Theft?*, 64 Hastings L.J. 1447 (2013).

Footnote 9: While this is not an issue raised by defendants on these motions, it is dispositive because the damages sought by plaintiff in the AC on its CFAA claim are not recoverable as a matter of law.

Footnote 10: Plaintiff does not claim that its database was itself damaged by virtue of defendants' alleged unauthorized access.

Footnote 11:A review of the cited case law makes clear that one reason courts interpret the statute narrowly is because unfair competition injuries are not recoverable under the CFAA. *See JBCHoldings NY, LLC v Pakter*, 931 FSupp2d 514, 524 (SDNY 2013) ("The Second Circuit's analysis there implicitly shows that the statute as a whole does not reach misappropriation of lawfully accessed information: **It would be illogical for the statute to prohibit misappropriation of employer information, but not to define loss to include the losses resulting from that misappropriation.**") (emphasis added). It is unclear why plaintiff did not plead (as opposed to simply note in its opposition brief) a cause of action for unfair competition, instead of tethering this claim to the CFAA. *See ITC Ltd. v Punchgini, Inc.*, 9 NY3d 467, 477-78 (2007) (explaining "the misappropriation theory of unfair competition.").

Footnote 12:"The SCA was meant 'to protect privacy interests in personal and proprietary information transmitted through then-emerging computer-based forms of communication.'" *In re 381 Search Warrants Directed to Facebook, Inc.*, 2017 WL 1216079 (Ct App Apr. 4, 2017) (citation and quotation marks omitted); *see Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 2017 WL 362765, at *2 (2d Cir Jan. 24, 2017) (Carney, J., concurring in denial of rehearing en banc) (noting that "the panel majority determined that the SCA's focus lies on protecting user privacy").

Footnote 13: This court's earlier decision on the motion to dismiss in *MSCI* did not dismiss the trade secrets claim and was affirmed by the Appellate Division (the court only dismissed the CFAA claim, under *Nosal I*, due to the mere claim that defendant violated his employer's terms of use). *See MSCI Inc. v Jacob*, 96 AD3d 637 (1st Dept 2012).

Footnote 14: Plaintiff's suggestion that the federal courts do not enforce the "consumer oriented" element is erroneous. *See Mount v PulsePoint, Inc.*, 2017 WL 1147191, at *2 (2d Cir Mar. 27, 2017).

Return to Decision List