



KeyCite Yellow Flag - Negative Treatment

Declined to Follow by [NetApp, Inc. v. Nimble Storage, Inc.](#), N.D.Cal.,
January 29, 2015

725 F.Supp.2d 887

United States District Court, N.D. California,
San Jose Division.

MULTIVEN, INC., Plaintiff,

v.

CISCO SYSTEMS, INC., Defendant.

Cisco Systems, Inc., et
al., Counterclaimants,

v.

Multiven, et al., Counterdefendants.

No. C 08–05391 JW

|

July 20, 2010.

Synopsis

Background: Former employee's company filed action against former employer, alleging that former employer violated Sherman Act by monopolizing and attempting to monopolize the market for provision and maintenance of network software. Former employer filed counterclaims alleging, inter alia, violation of the Computer Fraud and Abuse Act (CFAA), and violation of the California Unfair Competition Law (UCL). Parties filed cross-motions for partial summary judgment on the counterclaims.

Holdings: The District Court, [James Ware, J.](#), held that:

[1] former employee acted with “intent to defraud” within meaning of CFAA when he

accessed former employer's computer network with knowledge of former employer's policy prohibiting such access by non-employees;

[2] costs associated with investigating intrusions into a computer network and taking subsequent remedial measures were “losses” within the meaning of CFAA; and

[3] former employer had standing to pursue claim under UCL.

Counterclaimants' motion granted.

Procedural Posture(s): Motion for Summary Judgment.

West Headnotes (8)

[1] **Telecommunications** 🔑 Data breaches; hacking

Computers using network connected to the internet were “protected computers” within the meaning of Computer Fraud and Abuse Act (CFAA). 18 U.S.C.A. § 1030(e)(2) (B).

[27 Cases that cite this headnote](#)

[2] **Telecommunications** 🔑 Authorization or consent

Where employer had rescinded permission to access its computers after employee left his employment, any access by former employee to secure areas of former employer's computer network was “without

authorization” within meaning of Computer Fraud and Abuse Act (CFAA); since an employee's giving his login and password to former employee was a violation of employer's policies, and employee's providing access to former employee did not constitute a valid authorization. 18 U.S.C.A. § 1030(a)(4); 18 U.S.C.(2006 Ed.) § 1030(a)(5)(A)(iii).

12 Cases that cite this headnote

[3] Telecommunications 🔑 Data breaches; hacking

For purposes of Computer Fraud and Abuse Act (CFAA), “defraud” means wrongdoing and does not require proof of common law fraud; however, a plaintiff cannot prove “intent to defraud” by merely showing that an unauthorized access has taken place. 18 U.S.C.A. § 1030(a)(4); 18 U.S.C.(2006 Ed.) § 1030(a)(5)(A)(iii).

8 Cases that cite this headnote

[4] Telecommunications 🔑 Intent; willfulness

Former employee acted with “intent to defraud” within meaning of Computer Fraud and Abuse Act (CFAA) when he accessed former employer's computer network with knowledge of former employer's policy prohibiting such access by non-employees; even if former

employee genuinely believed that employee gave him authorization for a limited purpose on one occasion, there was no evidence that former employee had any reason to believe that having employee's login and password gave him unlimited authorization to access former employer's secure website at will. 18 U.S.C.A. § 1030(a)(4); 18 U.S.C.(2006 Ed.) § 1030(a)(5)(A)(iii).

1 Case that cites this headnote

[5] Telecommunications 🔑 Data breaches; hacking

Costs associated with investigating intrusions into a computer network and taking subsequent remedial measures were “losses” within the meaning of Computer Fraud and Abuse Act (CFAA). 18 U.S.C.A. § 1030(e)(11).

22 Cases that cite this headnote

[6] Telecommunications 🔑 Data breaches; hacking

Former employee violated California's counterpart to Computer Fraud and Abuse Act (CFAA) when he accessed former employer's computer network with knowledge of former employer's policy prohibiting such access by non-employees. 18 U.S.C.A. § 1030(a)(4); 18 U.S.C.(2006 Ed.) § 1030(a)

(5)(A)(iii); West's Ann.Cal.Penal Code § 502.

8 Cases that cite this headnote

[7] **Antitrust and Trade Regulation** 🗝️ Private entities or individuals

To have standing to bring a cause of action under California Unfair Competition Law (UCL), a plaintiff must show either prior possession or a vested legal interest in the money or property allegedly lost. 📄 West's Ann.Cal.Bus. & Prof.Code § 17200 et seq.

1 Case that cites this headnote

[8] **Antitrust and Trade Regulation** 🗝️ Private entities or individuals

Loss of valuable software and the considerable expense of investigating security breaches and possible compromise of the integrity of computer network constituted substantial economic loss for purposes of establishing standing to pursue claim under California Unfair Competition Law (UCL) based on unauthorized access to computer network. 📄 West's Ann.Cal.Bus. & Prof.Code § 17200 et seq.

1 Case that cites this headnote

Attorneys and Law Firms

*888 Donald Ross Pepperman, James Robert Noblin, Maxwell Michael Blecher, Blecher & Collins, Brian Curtis Vanderhoof, Thomas Michael O'Leary, Ropers Majeski, Kohn & Bentley, James C. Potepan, Attorney at Law, Los Angeles, CA, Charles F. Rule, Joseph J. Bial, Cadwalader Wickersham & Taft LLP, Washington, DC, for Plaintiff, Counterdefendants.

Patrick Martin Ryan, Krista M. Enns, John Caleb Donaldson, Winston & Strawn LLP, San Francisco, CA, Dan Keith Webb, Winston & Strawn LLP, Chicago, IL, for Defendant, Counterclaimants.

Michael Sungwoo Kim, Ropers, Majeski, Kohn & Bentley, Los Angeles, CA, for Counterdefendants.

ORDER GRANTING CISCO'S MOTION FOR PARTIAL SUMMARY JUDGMENT; DENYING MULTIVEN'S MOTION FOR PARTIAL SUMMARY JUDGMENT

JAMES WARE, District Judge.

Presently before the Court are Defendants and Counterclaimants Cisco Systems, *889 Inc. and Cisco Technology, Inc.'s (collectively, "Cisco") Motion for Partial Summary Judgment Against Counterdefendants Peter Alfred-Adekeye ("Adekeye") and Multiven, Inc. (collectively, "Multiven")¹ and Counterdefendants' Motion for Partial Summary Judgment.² The Court conducted a hearing on June 7, 2010. Based on the

papers submitted to date and oral argument, the Court GRANTS Cisco's Motion and DENIES Multiven's Motion.

A. Background

1. Undisputed Facts

Cisco Systems, Inc. is a leading provider of networking equipment (primarily switches and routers) and related services.³ Cisco Technology, Inc. is a wholly-owned subsidiary of Cisco Systems, Inc.⁴ Until May 2005, Adekeye was a Cisco employee. (Answer ¶¶ 45, 47.) During his employment with Cisco, Adekeye worked as a Technical Assistance Center (“TAC”) engineer. (*Id.* ¶ 45.)

On or about March 2, 2005, Adekeye incorporated Multiven. (Answer ¶ 48.) Multiven is a Delaware Corporation that purports to provide service and maintenance support for router and networking systems, including those placed in the market by Cisco.⁵ At all relevant times, Adekeye has been the CEO of Multiven. (*Id.* ¶ 49.)

2. Procedural History

On December 1, 2008, Multiven filed this action against Cisco alleging, *inter alia*, monopolization and attempted monopolization of the market for provision and maintenance of Cisco network software in violation of the Sherman Act, 15 U.S.C. § 2. (Complaint ¶¶ 17–61.) On November 20, 2009, Cisco filed a First Amended Answer and Second Amended Counterclaims alleging, *inter alia*, violation of the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, violation of

the California Penal Code § 502, and violation of the California Unfair Competition Law (“UCL”), Cal. Bus. & Prof.Code § 17200 *et seq.* (hereafter, “SAC,” Docket Item No. 59.)

Presently before the Court are the parties' Motions for Partial Summary Judgment.

B. Standards

Although motions for partial summary judgment are common, *890 Rule 56 of the Federal Rules of Civil Procedure, which governs summary judgment, does not contain an explicit procedure entitled “partial summary judgment.” However, partial summary judgment is inherent in that Rule 56(a) provided for summary judgment on “all or part of the claim.” Thus, a party may move for summary judgment on the liability issues in a claim, leaving the issue of damages, for example, for trial.

The purpose of summary judgment “is to isolate and dispose of factually unsupported claims or defenses.” *Celotex v. Catrett*, 477 U.S. 317, 323–24, 106 S.Ct. 2548, 91 L.Ed.2d 265 (1986). Thus, partial summary judgment may be used to dispose of a factually unsupported claim or affirmative defense.

As with a motion on the entire claim, under Rule 56(c), partial summary judgment is proper “if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment [on a part of the claim or an affirmative defense] as a matter of law.” Fed.R.Civ.P. 56(c). The moving

party “always bears the initial responsibility of informing the district court of the basis for its motion, and identifying the evidence which it believes demonstrates the absence of a genuine issue of material fact.” [🚩 *Celotex*, 477 U.S. at 323, 106 S.Ct. 2548](#). The non-moving party must then identify specific facts “showing a genuine issue for trial.” [Fed.R.Civ.P. 56\(e\)](#).

When evaluating a motion for partial or full summary judgment, the court views the evidence through the prism of the evidentiary standard of proof that would pertain at trial. [🚩 *Anderson v. Liberty Lobby Inc.*, 477 U.S. 242, 255, 106 S.Ct. 2505, 91 L.Ed.2d 202 \(1986\)](#). The court draws all reasonable inferences in favor of the non-moving party, including questions of credibility and of the weight that particular evidence is accorded. *See, e.g.*, [🚩 *Masson v. New Yorker Magazine, Inc.*, 501 U.S. 496, 520, 111 S.Ct. 2419, 115 L.Ed.2d 447 \(1991\)](#). The court determines whether the non-moving party's “specific facts,” coupled with disputed background or contextual facts, are such that a reasonable jury might return a verdict for the non-moving party. [🚩 *T.W. Elec. Serv. v. Pac. Elect. Contractors*, 809 F.2d 626, 631 \(9th Cir.1987\)](#). In such a case, partial summary judgment is inappropriate. [🚩 *Anderson*, 477 U.S. at 248, 106 S.Ct. 2505](#). However, where a rational trier of fact could not find for the non-moving party based on the record as a whole, there is no “genuine issue for trial.” [🚩 *Matsushita Elec. Indus. Co. v. Zenith Radio*, 475 U.S. 574, 587, 106 S.Ct. 1348, 89 L.Ed.2d 538 \(1986\)](#).

C. Discussion

1. Cisco's Motion re: the CFAA Claim

Cisco move for summary judgment on their CFAA claim on the ground that on multiple occasions and without authorization, Adekeye used a Cisco employee's password to gain access to Cisco's computer systems and download Cisco's proprietary and copyrighted software. (Cisco's Motion at 2.) Multiven respond that Adekeye only used a Cisco employee's password to access Cisco's computer systems once, and on that occasion he had the employee's permission to do so.⁶

The Ninth Circuit has explained the purpose of the CFAA as follows:

***891** The CFAA was enacted in 1984 to enhance the government's ability to prosecute computer crimes. The act was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to access and control high technology processes vital to our everyday lives. The CFAA prohibits a number of different computer crimes, the majority of which involve accessing computers without authorization or in excess of authorization, and then taking specified

forbidden actions, ranging from obtaining information to damaging a computer or computer data.

📌 *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1130–31 (9th Cir.2009) (internal quotation omitted).

Although Cisco's Counterclaim only alleges violation generally of 18 U.S.C. § 1030, and does not specify which subsections cover Adekeye's alleged actions,⁷ Cisco move for Summary Judgment pursuant to §§ 1030(a)(4) and 1030(a)(5)(A)(iii). (See Cisco's Motion at 11.) Thus, the Court only considers those two subsections for purposes of this Motion.

To successfully bring an action under § 1030(a)(4), a plaintiff must show that the defendant: (1) accessed a “protected computer,” (2) without authorization or exceeding such authorization that was granted, (3) “knowingly” and with “intent to defraud,” and thereby (4) “further[ed] the intended fraud and obtain[ed] anything of value,” causing (5) a loss to one or more persons during any one-year period aggregating at least \$5000 in value. See 18 U.S.C. § 1030(a)(4); 📌 *LVRC Holdings*, 581 F.3d at 1132.

To successfully bring an action under § 1030(a)(5)(A)(iii), a plaintiff must show that the defendant: (1) accessed a “protected computer,” (2) without authorization,⁸ (3) intentionally, and (4) “as a result of such conduct, cause[d] damage.”⁹

The Court addresses the elements necessary to establish liability under the CFAA in turn.

a. Protected Computer

At issue is whether Adekeye accessed a “protected computer,” as that term is defined under the statute.

The CFAA defines a “protected computer” as one “which is used in interstate or foreign commerce or communication.” 18 U.S.C. § 1030(e)(2)(B). The Ninth Circuit has found that “[a]s both the means to engage in commerce and the method by which transactions occur, the Internet is an instrumentality and channel of interstate commerce.” 📌 *United States v. Sutcliffe*, 505 F.3d 944, 953 (9th Cir.2007).

[1] Here, the parties do not dispute that Cisco's network is connected to the internet. (See Cisco's Motion at 12–13; Multiven's Opposition.) Thus, the Court *892 finds that computers using the Cisco network are “protected” within the meaning of the statute.

b. Without Authorization

At issue is whether Adekeye accessed secure areas of Cisco's network without authorization.

In the context of the CFAA, the Ninth Circuit has held that “a person uses a computer ‘without authorization’ ... when the person has not received permission to use the computer for any purpose ... or when the employer has rescinded permission to access the computer

and the defendant uses the computer anyway.”

🚩 *LVRC Holdings*, 581 F.3d at 1135.

[2] Here, Adekeye is a former employee of Cisco, however, there is no evidence that any privileges he had as an employee to access secure areas of the Cisco website extended beyond his employment. Cisco, however, has presented unrebutted evidence that upon leaving Cisco's employ, neither Adekeye nor Multiven had Cisco's permission or authorization to access Cisco's network. (Bouja Decl. ¶ 3.) Thus, the Court finds that any access by Adekeye to secure areas of the Cisco network was without authorization.



Multiven admit that on one occasion Adekeye accessed secure areas of the Cisco network. They contend however, that a Cisco employee, Wes Olson, supplied Adekeye with his login and password, thus authorizing Adekeye to access the restricted website. (Multiven's Opposition at 7–12.) It is undisputed that Wes Olson provided Adekeye with his login and “external” password. Olsen declares that the password was given to Adekeye “to give him access to Cisco's network on one occasion, for a specific purpose.”¹⁰ However, it is also undisputed that an employee's giving his login and password to Adekeye was a violation of Cisco's policies, and thus Olson's providing access to Adekeye in this manner did not constitute a valid authorization.

Accordingly, the Court finds that there is no genuine issue of material fact that Adekeye accessed secure areas of the Cisco server without authorization.

c. Knowledge and Intent

Cisco contend that Adekeye, without authorization, accessed Cisco's network “knowingly” and with “intent to defraud” within the meaning of the CFAA. (Cisco's Motion at 14–16.)

[3] Neither “knowingly” or “intentionally” are specifically defined by the CFAA. Thus, the court applies the “fundamental canon of statutory construction ... that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning.” 🚩 *Perrin v. United States*, 444 U.S. 37, 42, 100 S.Ct. 311, 62 L.Ed.2d 199 (1979). For purposes of the CFAA, “[t]he term ‘defraud’ ... simply means wrongdoing and does not require proof of common law fraud.” 🚩 *Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc.*, 556 F.Supp.2d 1122, 1131 (E.D.Cal.2008); *see also* 🚩 *eBay, Inc. v. Digital Point Solutions, Inc.*, 608 F.Supp.2d 1156, 1164 (N.D.Cal.2009). However, a plaintiff cannot prove “intent to defraud” by merely showing that an unauthorized access has taken place. 🚩 *P.C. Yonkers, Inc. v. Celebrations The Party and Seasonal Superstore, LLC*, 428 F.3d 504, 509 (3d Cir.2005). “Without a showing of some taking, or use, of information, it is difficult to prove intent to defraud.” *Id.* As the Ninth Circuit has recognized on numerous occasions, “[c]ases where intent is a primary issue generally are inappropriate for summary judgment unless all reasonable inferences that could be drawn *893 from the evidence defeat


the plaintiff's claims.”   *Provenz v. Miller*, 102 F.3d 1478, 1489 (9th Cir.1996).

[4] Here, Cisco present evidence that on multiple occasions, a person accessed the Cisco secure computer server from an IP address tied to Adekeye. (Bouja Decl. ¶¶ 4, 10.) Cisco further present evidence that Olson, a current Cisco employee who had an investment and business relationship with Adekeye, gave Adekeye his unique Cisco-issued user ID and external password.¹¹ In his declaration, Olson admits that giving Adekeye the password was a violation of Cisco's policies, and he states that based on conversations he had with Adekeye, Adekeye was aware of this fact. (*Id.* ¶ 3.)

Adekeye admits that on one occasion, he used Olson's password to access Cisco's secure network.¹² Adekeye declares that Olson “volunteered” the password, and that he never downloaded any Cisco software using Olson's password for use in his business. (*Id.*) As to his mental state at the time that he accessed Cisco's network, Adekeye declares,

Because Olson was a salesperson and/or manager for Cisco at the time he gave me his login and password information, I believed that he was authorized to do so. Olson was also heavily involved with sales and operations for Cisco at that time. Olson never told me what areas of Cisco's

website I could or could not access or for what purpose I could use his information. In fact, when Olson gave me his login and password information he did not give me any warning or instruction for its use.¹³

In response to Cisco's evidence that an individual using an IP address associated with Adekeye used Olson's password to access Cisco's network on multiple occasions, Multiven present evidence that throughout the time period in which the alleged invasions were taking place, Olson was a daily visitor to Adekeye's home, which then also served as the Multiven office. (Adekeye Opposition Decl. ¶¶ 3, 4.) According to Adekeye, Olson had access to the computers in Adekeye's home, and used them to remotely access the Cisco network. (*Id.* ¶ 4.) However, Cisco's undisputed evidence shows that during the time period in which the unauthorized accesses occurred from the IP address associated with Adekeye, Olson was traveling extensively out of the area.¹⁴ In the face of undisputed evidence that the Cisco network was accessed on multiple occasions from an IP address associated with Adekeye, along with the undisputed evidence that Olson provided Adekeye with his login *894 and password, Adekeye's self-serving testimony that he only accessed the secure website once cannot create a genuine triable issue of fact as to whether he only accessed the website on one occasion. See  *Kennedy v. Applause, Inc.*, 90 F.3d 1477, 1481 (9th Cir.1996) (refusing to find a “genuine issue” where the only evidence presented is “uncorroborated and self-serving”

testimony); [Villiarimo v. Aloha Island Air, Inc.](#), 281 F.3d 1054, 1061 (9th Cir.2002) (accord). Thus, the Court finds that there is no genuine issue of material fact that Adekeye accessed secure areas of the Cisco network on multiple occasions.

Given the number of times that Adekeye accessed the secure areas of the Cisco network, the Court finds that no reasonable juror could conclude that Adekeye actually believed that he had Cisco's authorization to do so. Even if Adekeye genuinely believed that Olson gave him authorization for a limited purpose on one occasion, there is no evidence that Adekeye had any reason to believe that having Olson's login and password gave him unlimited authorization to access Cisco's secure website at will. Furthermore, as a former Cisco employee, Adekeye cannot create a genuine issue of material fact as to his knowledge that he was entering areas of the Cisco network without authorization by merely claiming ignorance of Cisco's policy prohibiting such access for non-employees. (See Bouja Decl. ¶ 3.) Finally, Adekeye has admitted that his reason for accessing Cisco's secure website was to gather information about which Cisco employees have access to “bug fixes,” referring to Olson as a “whistleblower.”¹⁵ It is not within the realm of reason for Adekeye to have believed that Cisco would authorize one of its employees to provide his login and password to a purported competitor to carry out whistleblowing activities.

Accordingly, the Court finds that there is no genuine issue of material fact that Adekeye acted with the requisite mental state for liability

under the CFAA when he accessed Cisco's network.

d. Damage and Loss

At issue is whether Cisco have suffered damage or loss within the meaning of the statute.

[5] The CFAA defines “damage” as “any impairment to the integrity or availability of data, a program, a system or information.” 18 U.S.C. § 1030(e)(8). The CFAA defines “loss” as “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.” *Id.* § 1030(e)(11). Although the Ninth Circuit has not explicitly addressed the issue, district courts in the Ninth Circuit have held that it is not necessary for data to be physically changed or erased to constitute damage to that data. [Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.](#), 119 F.Supp.2d 1121, 1126–27 (W.D.Wash.2000); see also, e.g., [*895 Therapeutic Research Faculty v. NBTY, Inc.](#), 488 F.Supp.2d 991, 996 (E.D.Cal.2007). It is sufficient to show that there has been an impairment to the integrity of data, as when an intruder retrieves password information from a computer and the rightful computer owner must take corrective measures “to prevent the infiltration and gathering of confidential information.” [Shurgard](#), 119 F.Supp.2d at 1127. Costs associated with investigating

intrusions into a computer network and taking subsequent remedial measures are losses within the meaning of the statute. See [Kimberlite Corp. v. Does](#), 2008 WL 2264485, *1–2, 2008 U.S. Dist. LEXIS 43071, *4 (N.D.Cal.2008).

Here, Cisco present evidence that Cisco's operating software valued at over \$14,000 was subject to unauthorized downloads, resulting from unauthorized intrusions into Cisco's secure website originating from the IP address associated with Adekeye. (Bouja Decl. ¶ 17.) Adekeye's only response to this evidence of unauthorized downloads was his testimony that he “never downloaded any software using Wesley Kent Olson's password(s) for use in [his] business.” (Adekeye Decl. ¶ 6.) Adekeye did not deny using Olson's password to download software for purposes other than his business. Furthermore, Cisco present evidence that Cisco expended at least \$75,000 investigating the intrusions into their network and “restoring the security and integrity of Cisco's proprietary systems.” (*Id.*) Thus, the Court finds that there is no genuine issue of material fact that Adekeye's unauthorized access of Cisco's network caused Cisco damage and loss in excess of \$5000.

Since there are no genuine issues of material fact remaining as to the elements for liability under the CFAA, the Court GRANTS Cisco's Motion for Summary Judgment as to their claim under the CFAA.

2. Ciscos' Motion re: [California Penal Code § 502 Claim](#)

[6] Cisco move for summary judgment as to their claim under [California Penal Code § 502](#)

on essentially the same grounds as their claim under the CFAA. (Cisco's Motion at 12.)

[California Penal Code § 502\(c\)](#), the California corollary to the CFAA, provides, in pertinent part:

[A]ny person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.....

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

Here, Cisco's [Section 502](#) claim is based on the identical facts as their CFAA claim. Since the necessary elements of [Section 502](#) do not differ materially from the necessary elements of the CFAA for purposes of this action, the Court finds that there are no genuine issues of

material fact remaining as to Cisco [Section 502](#) claim.

***896** Accordingly, the Court GRANTS Cisco's Motion for Summary Judgment as to their claim under [Section 502\(c\)](#).

3. Multiven's Motion re: Cisco's UCL Claim

Multiven move for summary judgment as to Cisco's UCL claim on the ground that Cisco have suffered no injury in fact, and thus do not have standing to bring such a claim. (Multiven's Motion at 2.) Multiven contend that UCL standing is limited to individuals who suffer losses of money or property that are eligible for restitution.¹⁶ Cisco respond that eligibility for a restitutionary remedy is not a requirement for UCL standing, and Cisco's have adequately demonstrated that they suffered a loss.¹⁷

[7] The UCL prohibits “any unlawful, unfair or fraudulent business act or practice.”¹⁸ [Cal. Bus. & Prof.Code § 17200](#). To have standing to bring a cause of action under the UCL, a plaintiff must have “suffered injury in fact and [] lost money or property as a result of the unfair competition.” [Cal. Bus. & Prof.Code § 17204](#). More specifically, under [section 17204](#), a plaintiff must show “either prior possession or a vested legal interest in the money or property allegedly lost.” [Walker v. USAA Cas. Ins. Co.](#), 474 F.Supp.2d 1168, 1172 (E.D.Cal.2007), *aff'd*, [Walker v. Geico Gen. Ins. Co.](#), 558 F.3d 1025 (9th Cir.2009) (citing [Buckland v. Threshold Enters. Ltd.](#), 155 Cal.App.4th 798, 66 Cal.Rptr.3d 543 (Cal.Ct.App.2007)). As such, “[a]ny person

may pursue representative claims or relief on behalf of others only if the claimant meets the standing requirements of § 17204....” [Cal. Bus. & Prof.Code § 17203](#).

In a recent case, the Court found that standing under the UCL does not require a loss of money or property that is eligible for restitution.¹⁹ In that case, the Court followed Judge Chesney's reasoning in [Fulford v. Logitech, Inc.](#), to hold that a plaintiff has UCL standing if it alleges a loss of money or property in which it had prior possession or a vested legal interest, even if that loss is not eligible for restitution. [2009 WL 1299088 \(N.D.Cal. May 8, 2009\)](#). Multiven here do not cite any authority that would lead the Court to reconsider its prior holding in this regard.

As Multiven point out, the Ninth Circuit cited *Buckland* as authority for the proposition that UCL standing requires a showing of “lost money or property.” [Walker](#), 558 F.3d at 1027. In a parenthetical to the *Buckland* citation, the Ninth Circuit includes a quote from that case which states, “Because remedies for individuals under the UCL are restricted to injunctive relief and restitution, the import of the requirement is to limit standing to individuals who suffer losses of money or property that are eligible for restitution.” [Id.](#) However, the ***897** issue of availability of restitution was not before the Ninth Circuit in *Walker*, and thus its quotation of the language from *Buckland* was dicta. The district court in *Walker* only held that to have UCL standing, a plaintiff “must show either prior possession or a vested legal interest in money or property allegedly lost,” without addressing whether

such a loss implicates a restitutionary remedy.

[Walker](#), 474 F.Supp.2d at 1172.

[8] As previously discussed, Cisco present evidence that Cisco's operating software valued at over \$14,000 was subject to unauthorized downloads, allegedly resulting from Adekeye's invasion into Cisco's network, and that Cisco expended at least \$75,000 investigating the intrusions into their network and restoring the security of its systems. (Bouja Decl. ¶ 17.) The Court finds that Cisco have made a sufficient showing of a loss of money or property resulting from Adekeye's alleged invasions into Cisco's network to impart UCL standing. The loss of valuable software and the considerable expense of investigating security breaches and possible compromise of the integrity of the network constitute substantial economic loss. Moreover, prior to the alleged unauthorized download of Cisco's software, Cisco had possession of, and a vested legal interest in that software.²⁰

Accordingly, the Court DENIES Multiven's Motion for Partial Summary Judgment as to Cisco's UCL claim on the ground that Cisco have not adequately shown an injury in fact to impart standing.

4. Multiven's Motion to Stay

On June 8, 2010, Multiven filed a Motion to Stay Counterclaims. (hereafter, "Motion to Stay," Docket Item No. 234.) Multiven contend that further litigation of the counterclaims will jeopardize Adekeye's Fifth Amendment privileges in parallel criminal proceedings arising out of the same factual circumstances. (Motion to Stay at 5–7.) Multiven further

contend that the factors recognized by the Ninth Circuit in [Keating v. Office of Thrift Supervision](#), 45 F.3d 322, 324 (9th Cir.1995), for determining whether a stay is appropriate weigh in favor of a stay here. (*Id.* at 8–10.)

Here, Adekeye has already voluntarily submitted declarations in support of Multiven's briefs regarding the parties' cross-motions for summary judgment and has been deposed extensively, including fourteen hours of deposition testimony that he voluntarily provided in Vancouver, Canada prior to his arrest. Without deciding whether Adekeye was sufficiently aware of the likelihood of criminal prosecution for his declarations and deposition testimony to effect a waiver of his Fifth Amendment rights,²¹ the Court finds that continuing the litigation will only minimally implicate Adekeye's Fifth Amendment rights, given the extensive testimony he has already provided in this case. See [F.T.C. v. J.K. Publ'ns, Inc.](#), 99 F.Supp.2d 1176, 1199 (C.D.Cal.2000) ("Where a defendant already has provided deposition testimony on substantive issues of the civil case, any burden on that defendant's Fifth Amendment privilege is 'negligible.'"). As to the remaining *Keating* balancing test factors, the Court finds that the burden on Adekeye *898 of proceeding with the counterclaims does not outweigh the burden on Cisco of proceeding with Multiven's antitrust claims while its counterclaims are stayed. Further, neither the convenience of the Court nor the interests of the public will be served by a stay.

Accordingly, the Court DENIES Multiven's Motion to Stay Counterclaims.

D. Conclusion

The Court GRANTS Cisco's Motion for Partial Summary Judgment as to Cisco's claims under the CFAA and [California Penal Code § 502](#). The Court DENIES Multiven's Motion for Partial Summary Judgment as to Cisco's UCL claim.

The Court DENIES Multiven's Motion to Stay Counterclaims.

All Citations

725 F.Supp.2d 887

Footnotes

- 1 (hereafter, "Cisco's Motion," Docket Item No. 111, redacted public version; Docket Item No. 134, seal version.)
- 2 (hereafter, "Multiven's Motion," Docket Item No. 108.)
- 3 (Declaration of Alex T. Bouja in Support of Motion of Cisco Systems, Inc. and Cisco Technology, Inc. for Partial Summary Judgment Against Peter Alfred–Adekeye and Multiven, Inc., hereafter, "Bouja Decl.," Docket Item No. 112, redacted public version.) Multiven have filed extensive objections to the Declaration of Mr. Bouja. (See Defendants' Evidentiary Objections to the Declaration of Alex T. Bouja and Exhibits Thereto Submitted in Support of Plaintiff's Motion for Partial Summary Judgment Against Peter Alfred–Adekeye and Multiven, hereafter, "Objections," Docket Item No. 163.) Upon review of the Declaration of Mr. Bouja, the Court finds that Mr. Bouja has sufficiently demonstrated that he has personal knowledge of the matters about which he attests. As Cisco's Program Manager of Legal Investigations, Mr. Bouja may testify to the nature of the investigation that Cisco undertook and the information that Cisco gleaned as a result of that investigation. Accordingly, the Court OVERRULES Multiven's Objections for the purposes of these Motions.
- 4 (Answer to the Second Amended Counterclaims ¶ 23, hereafter, "Answer," Docket Item No. 73.)
- 5 (Civil Complaint for Damages and Injunctive Relief, hereafter, "Complaint," Docket Item No. 1.)
- 6 (Opposition to Cisco Systems, Inc.'s Motion for Partial Summary Judgment Against Peter Alfred–Adekeye at 4, hereafter, "Multiven's Opposition," Docket Item No. 162, redacted version.)

- 7 (See SAC ¶¶ 123–31.)
- 8 In their statement of the elements of § 1030(a)(5)(A)(iii), Cisco add the term “exceeding such authorization that was granted” to the statutory language “without authorization.” (See Cisco's Motion at 11.) The Court finds that unlike § 1030(a)(4), § 1030(a)(5)(A)(iii) does not contain the phrase “exceeding such authorization that was granted.”
- 9 Since the CFAA is primarily a criminal statute, and §§ 1030(a)(4) and 1030(a)(5)(A)(iii) create criminal liability for violators of the statute, the Court applies the version of the CFAA that was in effect at the time that Adekeye allegedly committed the wrongs. See [LVRC Holdings](#), 581 F.3d at 1134; *U.S. v. Davidson*, 246 F.3d 1240, 1248 (9th Cir.2001). Pursuant to [Fed.R.Evid. 201](#), the Court takes judicial notice of the version of the statute pre-dating the 2008 amendments to the CFAA, which Cisco provide as Exhibit A to their Motion.
- 10 (Declaration of Kent Olson ¶ 3, hereafter, “Olson Decl.,” Docket Item No. 113.)
- 11 (Olson Decl. ¶¶ 3, 14.)
- 12 (Declaration of Peter Alfred–Adekeye in Support of Motion for Partial Summary Judgment ¶ 6, hereafter, “Adekeye Decl.,” Multiven's Motion, Ex. 1.)
- 13 (Declaration of Peter Alfred–Adekeye Opposition Motion by Cisco Systems, Inc. and Cisco Technology, Inc. for Partial Summary Judgment ¶ 6, hereafter, “Adekeye Opposition Decl.,” Multiven's Opposition, Ex. 1.)
- 14 Cisco's un rebutted evidence shows that Olson was in India from November 6–12, 2005; in Illinois from April 30–May 3, 2007; in Washington, D.C. from June 12–16, 2007; in Southern California from March 9–19, 2007; and on one occasion, he was logged into the Cisco network from a neighboring city while the use at the IP address associated with Adekeye was also logged in. (Declaration of Patrick M. Ryan in Support of Cisco's Reply in Support of its Motion for Partial Summary Judgment Against Peter Alfred–Adekeye and Multiven, hereafter, “Ryan Decl.,” Ex. A at 58:21–59:5, 59:6–14, 59:18–60:1, 65:11–67:20, Docket Item No. 177; Bouja Decl. ¶ 16(d), Ex. J; Supplemental Declaration of Alex T. Bouja in Support of Motion of Cisco Systems, Inc. and Cisco Technology, Inc. for Partial Summary Judgment Against Peter Alfred–Adekeye and Multiven, Inc. ¶¶ 17–19, Exs. KLM, Docket Item No. 176.)
- 15 (See, e.g., Adekeye Decl. ¶ 6 (“When I accessed Cisco's website on that one occasion, it was only to confirm amongst other things that it was not only Cisco's engineers that had access to the bug fix page but also its non-technical managers and salespeople.”); Adekeye Deposition Transcript, Vol. 2 at 525:12–15 (“So

Mr. Olson acting in whistleblower capacity volunteered information, and he even volunteered, without being asked, his username and password for his Cisco.com website....”), Declaration of Patrick M. Ryan in Support of Cisco's Opposition to Multiven's Motion to Stay Counterclaims, Ex. B, Docket Item No. 259.)

- 16 (Reply to Opposition to Multiven's Motion for Partial Summary Judgment at 2–9, hereafter, “Multiven's Reply,” Docket Item No. 174.)
- 17 (Cisco's Opposition to Multiven's Motion for Partial Summary Judgment at 4–6, hereafter, “Cisco's Opposition,” Docket Item No. 164.)
- 18 The California Supreme Court has stated that “the primary form of relief available under the UCL to protect consumers from unfair business practices is an injunction, along with ancillary relief in the form of such restitution ‘as may be necessary to restore to any person in interest any money or property, real or personal, which may have been acquired by means of such unfair competition.’ ” [In re Tobacco II Cases](#), 46 Cal.4th 298, 93 Cal.Rptr.3d 559, 207 P.3d 20 (2009) (quoting [§ 17203](#)).
- 19 (Order Granting in Part and Denying in Part Defendants' Motion to Dismiss; Denying Motion to Strike, Case No. C 08–5562 JW, Docket Item No. 23.)
- 20 The Court notes that even if eligibility for a restitutionary remedy were a prerequisite for UCL standing, Cisco's showing of loss would still be sufficient. Specifically, Cisco have presented evidence that Adekeye took Cisco's property, in the form of software downloads, without permission. In the event that Cisco were successful in proving that Adekeye took such action, an appropriate remedy would be return of the unlawfully downloaded software to Cisco.
- 21 see [Brown v. United States](#), 356 U.S. 148, 78 S.Ct. 622, 2 L.Ed.2d 589 (1958).