Vaquero Energy, Inc. v. Herda et al Doc. 43

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

VAQUERO ENERGY, INC., Plaintiff, v. JEFF HERDA, et al., Defendants.	Case No.: 1:15-cv-0967 - AWI - JLT ORDER GRANTING IN PART DEFENDANTS' MOTION TO DISMISS (Doc. 27)

Plaintiff Vaquero Energy, Inc., operates oil and gas collection and installations in California, Texas, Colorado, and Wyoming. Plaintiff contracted with Defendants to provide "[i]nformation technology maintenance, updates, upgrades and coordination services for oil and gas collection facility software, hardware and/or firmware." (Doc. 16 at 3-4) On August 20, 2015, Defendants filed a motion to dismiss Plaintiff's claims under the Computer Fraud and Abuse Act and the Stored Communications Act pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure. (Doc. 27) Plaintiff filed its opposition to the motion on September 3, 2015 (Doc. 40), to which Defendants filed a reply on September 14, 2015 (Doc. 41).

The Court heard the oral arguments of the parties at a hearing held on September 21, 2015. For the following reasons, Defendants' motion is **GRANTED IN PART**.

I. Background and Plaintiff's Allegations

Vaquero hired Jeff Herda in 2008 to provide the following services: "Information technology

Dockets.Justia.com

maintenance, updates, upgrades and coordination services for oil and gas collection facility software, hardware and/or firmware (combination of hardware and embedded software; e.g., mobile phones or digital cameras) including but not limited to Vaquero finance, operational and administrative software and systems, programmable logic controllers [PLC's] and a related centralized supervisory control and data acquisition [SCADA] system." (Doc. 16 at 3-4, ¶ 10) Plaintiff alleges the services involved "the translation of instructions received from plaintiff Vaquero's employees into a so-called ladder logic, whereby Defendants utilized third-party software… to select from a drop-down menu a series of instructions to establish a desired sequence to control and instruct effectively the PLC devices connected to oil and gas collection facilities." (Id. at 4, ¶ 11)

Plaintiff asserts that in 2014, Vaquero "initiated a restructuring of its information technology requirements, staffing and strategy." (Doc. 16 at 5, ¶ 15) Plaintiff alleges that prior to the restructuring, Defendants used a single password … for certain steam generators that was provided to, and known by, plaintiff Vaquero employees." (Id.) However, after the restructuring, Vaquero discovered the password "was no longer valid." (Id.) Plaintiff alleges, that unknown to Vaquero "and without permission or authorization, Defendants accessed [the] computer system and imposed new passwords and access control limitations on key or critical PLC devices, SCADA system, and central Vaquero operations and administrative software, hardware, firmware and systems." (Id.)

Plaintiff alleges that in December 2014, Plaintiff requested Herda provide all "logins and passwords to the various server, firewalls, and any other devices." (Doc. 16 at 6, ¶ 15(A)) In response, Herda provided "an Excel® spreadsheet which did not include or identify all requested information, or the information was inaccurate and did not allow access to various systems." (Id.) According to Plaintiff, on March 31, 2015, "Herda met with plaintiff Vaquero employees to discuss Vaquero's needs and strategy for information technology." (Doc. 16 at 6, ¶15(B)) Plaintiff asserts that at the meeting, the Vaquero employees again requested Herda provide "documentation files for the PLC ladder logic and all user names, passwords and access controls for all Vaquero, PLC's SCADA, and other software and systems." (Id.)

Vaquero asserts the information was not provided, and Seth Hunter (the Operations Manager) made another request for "passwords and documentation files" during a telephone conversation with

Herda in May 2015. (Doc. 16 at 6, ¶15(C)) Plaintiff contends that Herda refused to disclose the information, and "demanded … a license agreement by which plaintiff Vaquero would be required to pay to defendant Herda an unspecified license fee." (Id.) Further, Plaintiff asserts that Defendants "without authority deleted and modified the Passwords, ladder logic and/or data previously installed and activated on those PLC's … for the purpose of preventing plaintiff Vaquero's use and access to its own systems, computers and files." (Id. at 9, ¶ 18) Plaintiff alleges Defendants stopped providing services to Vaquero in May 2015, by which time Vaquero paid Defendants more than $1.3 million for the services rendered. (Id. ¶¶ 15, 16)

According to Vaquero, if the company "does not receive user names, passwords, control access information and documentation for all its PLC's, SCADA, and other software and systems, it will be unable to completely or effectively maintain, update, upgrade, add, remove and/or coordinate those devices, software and systems." (Doc. 16 at 8, ¶ 17) Consequently, Vaquero alleges that "the integrity, safety and security of plaintiff Vaquero's gas and oil collection installations, and all employees at those installations, are in jeopardy of a singular (or cascade of) failure(s) of the device(s), software and system(s) that may cause (a) mechanism(s) to malfunction – at a potentially catastrophic level."[1] (Id. at 8-9, ¶ 17)

Based upon these facts, Plaintiff alleges Defendants are liable for violations of (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) the California Computer Data Access and Fraud Act, Cal. Pen. Code §502; (3) the Stored Communications Act, 18 U.S.C. § 2701; and (4) California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200. (See generally Doc. 16) Here, Defendants seek dismissal of the first and third causes of action. (Doc. 27 at 1-2)

III. Legal Standards for a Motion to Dismiss

A Rule 12(b)(6) motion "tests the legal sufficiency of a claim." Navarro v. Block, 250 F.3d 729, 732 (9th Cir. 2001). Dismissal under Rule 12(b)(6) is appropriate when "the complaint lacks a cognizable legal theory or sufficient facts to support a cognizable legal theory." Mendiondo v.

[1] Vaquero requested a preliminary injunction to compel Defendants to disclose "passwords, user-names, .dat files, and all related access controls for all Vaquero computers, servers, and/or firmware and related attached equipment and components," and to enjoin Defendants from any further access of the PLCs and SCADA systems. (Doc. 15 at 2-3) The Court granted the preliminary injunction on August 28, 2015. (Docs. 34, 39)

Centinela Hosp. Med. Ctr., 521 F.3d 1097, 1104 (9th Cir. 2008). Thus, under Rule 12(b)(6), "review is limited to the complaint alone." Cervantes v. City of San Diego, 5 F.3d 1273, 1274 (9th Cir. 1993).

Allegations of a complaint must be accepted as true when the Court considers a motion to dismiss. Hospital Bldg. Co. v. Rex Hospital Trustees, 425 U.S. 738, 740 (1976). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)). The Supreme Court explained,

> A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. The plausibility standard is not akin to a "probability requirement," but it asks for more than a sheer possibility that a defendant has acted unlawfully. Where a complaint pleads facts that are "merely consistent with" a defendant's liability, it "stops short of the line between possibility and plausibility of 'entitlement to relief.'"

Iqbal, 556 U.S. at 678 (internal citations, quotation marks omitted).

A court must construe the pleading in the light most favorable to the plaintiff, and resolve all doubts in favor of the plaintiff. Jenkins v. McKeithen, 395 U.S. 411, 421 (1969). "The issue is not whether a plaintiff will ultimately prevail, but whether the claimant is entitled to officer evidence to support the claims. Indeed it may appear on the face of the pleadings that a recovery is very remote and unlikely but that is not the test." Scheuer v. Rhodes, 416 U.S. 232, 236 (1974). However, the Court "will dismiss any claim that, even when construed in the light most favorable to plaintiff, fails to plead sufficiently all required elements of a cause of action." Student Loan Marketing Assoc. v. Hanes, 181 F.R.D. 629, 634 (S.D. Cal. 1998). Leave to amend should not be granted if "it is clear that the complaint could not be saved by an amendment." Livid Holdings Ltd. v. Salomon Smith Barney, Inc., 416 F.3d 940, 946 (9th Cir. 2005).

IV. Request for Judicial Notice

In considering a motion to dismiss, the Court may consider material outside the pleadings when it is properly the subject of judicial notice. See Lee v. City of Los Angeles, 250 F.3d 668, 689 (9th Cir. 2001); MGIC Indemnity Corp. v. Weisman, 803 F.2d 500, 504 (9th Cir. 1986). The Court may take judicial notice of a fact that "is not subject to reasonable dispute because it (1) is generally known within the trial court's territorial jurisdiction; or (2) can be accurately and readily determined from

sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201.

Here, Defendants request that the Court take judicial notice of the declarations of Seth Hunter, Don Lawson, Mark Creasey, and Wyatt Shipley. (Doc. 29 at 1-2) However, Defendants fail to show the statements made by these individuals are subject to judicial notice. To the contrary, the statements made are subject to reasonable dispute, and many statements made by Vaquero's employees are, in fact, disputed by Defendants. Therefore, Defendants' request for judicial notice is **DENIED**.

V. Discussion and Analysis

Defendants seek dismissal of Plaintiff's claims arising under the Computer Fraud and Abuse Act and the Stored Communications act, asserting Vaquero fails to state cognizable claims under these acts because "defendants' conduct was authorized, and because plaintiff's computers and servers do not fall within the definition of electronic storage or electronic communication service facilities, as required by the Stored Communications Act." (Doc. 27 at 1-2)

A. Computer Fraud and Abuse Act, 18 U.S.C. §1030

Congress enacted the Computer Fraud and Abuse Act ("CFAA") "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." LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1131 (9th Cir. 2009) (internal quotation marks, citation omitted). "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." Id. (citing 18 U.S.C. § 1030(a)(1)-(7)).

The term "without authorization" is undefined, but the Ninth Circuit has determined that a person uses a computer "without authorization" under the CFAA "when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the [computer's owner] has rescinded permission to access the computer and the defendant uses the computer anyway." LVRC Holdings LLC, 581 F.3d at 1135. To exceed authorized access "means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18

U.S.C. § 1030(e)(6); see also LVRC Holdings LLC, 581 F.3d at 1133 ("an individual who is authorized to use a computer for certain purposes but goes beyond those limitations is considered by the CFAA as someone who has 'exceed[ed] authorized access'"). Here, Plaintiff asserts Defendants violated Sections 1030(a)(5) and 1030(a)(7). (Doc. 16 at 10)

1. Section 1030(a)(5)

Pursuant to this section, an individual violates the CFAA when he or she:

> (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
>
> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss[.]

18 U.S.C. § 1030(a)(5). Under the CFAA, "damage means any impairment to the integrity or availability of the data, a program, a system, or information[.]" Id., § 1030(e)(8). Therefore, there are two possible kinds of damage: damage resulting from impairment to the integrity of the data, program or system; and damage resulting from the inability to access the identified data, program, system, or information.

Plaintiff alleges its computers and servers "store its confidential information" and are 'protected computers' within the scope of 18 U.S.C. § 1030(e)(2)." (Doc. 16 at 10) In addition, Plaintiff alleges Defendants "intentionally accessed Vaquero's computers and servers and without authorization have intentionally locked Vaquero out of the use of those computers and servers." (Id.) Specifically, Plaintiff asserts Defendants accessed "Vaquero's Tunnell Master PLC and Ardantz Pad C PLC and, approximately between May 5, and May 15, 2015, without authority deleted and modified the Passwords, ladder logic and/or data previously installed and activated on those PLC's on May 5, 2015 for the purpose of preventing plaintiff Vaquero's use and access to its own systems, computers and files." (Id.) In addition, Plaintiff alleges Defendants changed the passwords to its five steam generators. (Id.) Because Plaintiff alleges Defendants were not authorized to modify the passwords or delete ladder logic, Plaintiff alleges facts sufficient to support a determination that Defendants intentionally accessed Vaquero's systems and exceeded the scope of the authorization to access the systems.

2. Section 1030(a)(7)

Plaintiff alleges Defendants violated this section of the CFAA, which provides a cause of action against an individual who "with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion"

18 U.S.C. § 1030(a)(7).

As discussed above, Vaquero asserts Defendants changed the passwords to the PLCs, and seems to suggest this was for the purpose of extorting money from the company. (See Doc. 16 at 10) However, Plaintiff fails to allege Defendants made any threats[2] to Vaquero, or made demands that were transmitted "in interstate or foreign commerce." Plaintiff alleges its counsel "delivered a demand" requesting the passwords and other data and, in response, Defendants "replied." (Doc. 16 at 7) Finally, Vaquero fails to allege facts to support a conclusion that the passwords were, in fact, changed for the purpose of extorting money, rather than protecting the copyright interest claimed by Defendants. Consequently, Plaintiff fails to state a cognizable claim under Section 1030(a)(7).

3. Damages or loss

In addition to imposing criminal penalties for the prohibited conduct, the CFAA creates a private right of action for "[a]ny person who suffers damage or loss by reason of a violation" of the statute. 18 U.S.C. § 1030(g). However, a private claim "may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)." Id. Thus, it is not enough that Plaintiff be able to show Defendants acted without authorization, or beyond the scope of authorization. To state a claim under the CFAA, a plaintiff must further show one of the following:

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a

[2] Seemingly, at issue in the first amended complaint, are the acts of Defendants taken to install passwords on the PLCs and other equipment certain when Defendants were authorized to access Plaintiff's system.

related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

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

(III) physical injury to any person;

(IV) a threat to public health or safety;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

(VI) damage affecting 10 or more protected computers during any 1-year period[.]

18 U.S.C. § 1030(c)(4)(A)(i).

In this case, Plaintiff alleges Vaquero incurred "substantial costs in excess of $5,000 to investigate and attempt to remediate" the actions taken by Defendants, including password-protecting the PCL and SCADA systems. (Doc. 16 at 10-11) Thus, Plaintiff has alleged damages sufficient to support a claim for relief under CFAA. However, Plaintiff fails to allege sufficient facts to support its CFAA claim premised upon Section 1030(a)(7). Accordingly, Defendants' motion to dismiss the first cause of action is **GRANTED IN PART**, and the claim, to the extent it is based upon Section 1030(a)(7), is dismissed with leave to amend.

B. Stored Communications Act, 18 U.S.C. § 2701

Vaquero asserts Defendants are liable for a violation of the Stored Communications Act ("SCA"), which creates criminal and civil liability for some acts of unauthorized access to wire and electronic communications and records in temporary and backup storage. See Knopp v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002). The SCA creates a private right of action against "whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in storage in such system…"

18 U.S.C. § 2701(a); see also 18 U.S.C. § 2707 (creating a private right of action).

The SCA defines the term "electronic communication services" as "any service which provides

to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Likewise, the SCA defines "electronic communications" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce [with four irrelevant exceptions]." 18 U.S.C. § 2510(12). The SCA does not define the term "facility." However, courts have determined that a "facility" is operated by electronic communication service providers. Cousineau v. Microsoft Corp., 6 F. Supp. 3d 1167, 1174 (W.D. Wash. 2014).

In Cousineau, the court determined whether a smart phone was a "facility" for purposes of the SCA. In relying heavily on In re iPhone Application Litigation, 844 F.Supp.2d, 1040, 1050 (N.D. Cal. 2012), Cousineau rejected that the smart phone was a facility when it held that, "The fact that the phone not only received but also sent data does not change this result, because nearly all mobile phones transmit data to service providers." Notably, cases after iPhone—as noted in Cosineau—determined that for a device to be a "facility" under the SCA, "it must perform server-like functions." For example, in In re Pharmatrak, Inc. Privacy Litig., 220 F. Supp. 2d 4, 13 (D. Mass. 2002) the Court explained,

> Defendants are correct that an individual Plaintiff's personal computer is not a "facility through which an electronic communication service is provided" for the purposes of § 2701. Plaintiffs find it noteworthy that "[p]ersonal computers provide consumers with the opportunity to access the Internet and send or receive electronic communications," and that "[w]ithout personal computers, most consumers would not be able to access the Internet or electronic communications." Fair enough, but without a telephone, most consumers would not be able to access telephone lines, and without televisions, most consumers would not be able to access cable television. Just as telephones and televisions are necessary devices by which consumers access particular services, personal computers are necessary devices by which consumers connect to the Internet. While it is possible for modern computers to perform server-like functions, there is no evidence that any of the Plaintiffs used their computers in this way. **While computers and telephones certainly provide services in the general sense of the word, that is not enough for the purposes of the ECPA. The relevant service is Internet access, and the service is provided through ISPs or other servers, not though Plaintiffs' PCs**.

Id. 220 F. Supp. 2d 4, 13 (D. Mass. 2002) (emphasis added); See also Theofel v. Farey-Jones, 359 F.3d 1066, 1071 (9th Cir. 2004) [pleading is sufficient if the "substance of plaintiffs' claims is that defendants improperly accessed [the defendant's] servers."]

Here, though Plaintiff alleges Defendants exceeded the scope of the authorization given to

access the PLCs and SCADA systems, Plaintiff fails to allege facts sufficient to support a conclusion that the PLCs and SCADA systems are "facilities" under the SCA. Consequently, Defendants' motion to dismiss the third cause of action is **GRANTED**, and the claim is dismissed with leave to amend.

VI. Conclusion and Order

Based upon the foregoing, **IT IS HEREBY ORDERED** that Defendants' motion to dismiss is **GRANTED IN PART**, as follows:

1. Defendants' motion to dismiss the first cause of action for a violation of the Computer Fraud and Abuse Act is **DENIED** to the extent it is based upon a violation of Section 1030(a)(5) and **GRANTED** to the extent the cause of action is based upon a violation of Section (a)(7);
2. Defendants' motion to dismiss the third cause of action for a violation for the Stored Communications Act is **GRANTED**; and
3. Plaintiff **SHALL** file any amended complaint **no later than September 21, 2015** of the date of service of this order. If Plaintiff chooses to not file a Second Amended Complaint, the First Amended Complaint will stand, with the claims dismissed as identified by this Order.

IT IS SO ORDERED.

Dated: **September 21, 2015**

/s/ Jennifer L. Thurston
UNITED STATES MAGISTRATE JUDGE