UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

VAQUERO ENERGY, INC., Plaintiff, v. JEFF HERDA, an individual and doing business as INTEGRATED CONTROL SYSTEMS, BRAXBRO, INC., a Nevada corporation and doing business as INTEGRATED CONTROL SYSTEMS, a corporation, Defendants.	Case No. 1:15-cv-0967 -JLT ORDER GRANTING PLAINTIFF'S MOTION FOR A PRELIMINARY INJUNCTION (Doc. 14)

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) Plaintiff asserts Defendants created user names, passwords and other access controls for the software, hardware and systems, but has not provided the information Plaintiff requested after the termination of their services. Plaintiff contends that if it "does not receive the user names, passwords, control access information and documentation for all . . . software and systems, it will be unable to completely or effectively maintain, update, upgrade, add, remove and/or coordinate those devices, software and systems." (Id. at 8) Therefore, Plaintiff seeks a preliminary injunction pursuant to Rule 65 of the Federal Rules of Civil Procedure

against Defendants, requesting that the Court enjoin Defendants from accessing Plaintiff's systems and order Defendant to return "any and all system structure, data, documents, software, files and/or folders that [Defendants] … downloaded, otherwise copied, or in any way received from Vaquero." (Doc. 14)

Defendants oppose the motion, arguing a mandatory injunction is not appropriate because Vaquero fails to show it is likely to suffer irreparable injury. Further, Defendants assert that Plaintiff is not likely to succeed on the merits of its claims. (Doc. 20)

The Court heard the oral arguments of the parties on August 26, 2015. For the following reasons, Plaintiff's motion for a preliminary injunction is **GRANTED**.

I. Background and Procedural History

Vaquero hired Jeff Herda in 2008 to provide the following services: "Information technology 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) When Plaintiff hired Herda, "Herda and ICS inherited the ladder logic, data and documents from Vaquero and its previous Santa Maria PLC/SCADA consultant, AC Electric, and from MC Automated for operation of the Steam Generators. Herda and ICS simply copied and modified that ladder logic and data and incorporated it into the current ladder logic and data." (Doc. 14-1 at 3, ¶ 4) Thus, Herda "incorporated the translation of instructions received from plaintiff Vaquero's employees into a so-called ladder logic," and to do so Defendants used 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) The reason Plaintiff required Herda "to maintain [Plaintiff's] programs and the language (ladder logic) written into [their] PLC's and other devices [was] so that another programmer could access and understand what the ladder logic contained. I knew that Herda was the only person employed by his company, it was very important to insulate our investment." (Doc. 14-1 at 4 ¶ 9)

Plaintiff asserts that "[e]ach PLC and SCADA device, software and hardware may be controlled via third-party software (RSLogix™, Wonderware® or others) to create and require security access including user names, passwords and other access control." (Doc. 16 at 5, ¶ 12) Vaquero alleges the "access control prohibits any modification of control and instructions to the PLC devices or the SCADA monitoring systems." (Id.) Plaintiff alleges it paid Defendants approximately $1,347,560.46 for the services rendered through May 2015. (Id., ¶14)

In late 2014, "Vaquero initiated a restructuring of its information technology requirements, staffing and strategy." (Doc. 16 at 5, ¶ 15) Prior to the restructuring, Vaquero had "a single password … for certain steam generators." (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)) According to Plaintiff, 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.)

On March 31, 2015, Herda met with Vaquero employees—including Seth Hunter, the Operations Manager of Vaquero; Don Lawson, the IT Administrator; and Wyatt Shipley, the Operations Engineer. (Doc. 16 at 6; Doc. 14-1 at 5, Hunter Decl. ¶ 14) Plaintiff asserts that at the meeting, the Vaquero employees 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." (Doc. 16 at 6, ¶15(B)) Defendant contends the Vaquero "representatives requested only the PLC 'documentation and programs.'" (Doc. 22 at 6, Herda Decl. ¶ 28) Although Plaintiff asserts Herda indicated he would provide this information, Herda contends he "neither agreed nor refused to provide the documentation and programs" during the meeting (*Compare* Hunter Decl. ¶ 14 *with* Herda Decl. ¶ 28).

According to Hunter, he "again requested the passwords and related information during a phone

call directly with Herda on May 1st 2015." (Doc. 14-1 at 6, ¶ 15) Hunter reports that Herda "refused and indicated that there would be a fee to access the PLCs." (Id.) Further, Plaintiff asserts, "Herda refused, before and after the termination of [Integrated Control Systems'] services, to provide all information, documentation, and passwords for all access into the noted PLCs and SCADA system." (Id., ¶ 16) In this motion, Plaintiff seeks to compel Herda to provide "any and all system structure, data, documents, software, files and/or folders that Herda and/or ICS downloaded," and to produce any "passwords, user-names, .dat files, and all related access controls for all Vaquero computers, servers, and/or firmware and related attached equipment and components (including, without limitation PLC's and SCADA system(s))." (Doc. 15 at 2-3)

II. Preliminary Injunctions

"The purpose of preliminary injunction is merely to preserve the relative position of the parties until a trial on the merits can be held." Univ. of Texas v. Camenisch, 451 U.S. 390, 395 (1981). A preliminary injunction may be either mandatory or prohibitory. See Rouser v. White, 707 F.Supp.2d 1055, 1061 (E.D. Cal. 2010). In general, a mandatory injunction is one that orders a party to "take action," while a prohibitory injunction is one that "restrains" a party from further action. Meghrig v. KFC Western, Inc., 516 U.S. 479, 484 (1996). Importantly, while a prohibitory injunction preserves the status quo, a mandatory injunction goes well beyond maintaining the status quo pending litigation. Stanley v. University of S. Cal., 13 F.3d 1313, 1320 (9th Cir. 1994). Because mandatory injunctions do not only preserve the status quo, they are "particularly disfavored," and the Ninth Circuit observed that "courts should be *extremely cautious* about issuing a preliminary injunction." Martin v. Int'l Olympic Committee, 740 F.2d 670, 675 (9th Cir. 1984) (emphasis added). The Court should deny request for a mandatory injunction "'unless the facts and law clearly favor the moving party.'" Stanley, 13 F.3d at 1320 (quoting Anderson v. United States, 612 F.2d 1112, 1114 (9th Cir. 1979)). Here, Plaintiffs seek a preliminary injunction compelling Defendants to produce the passwords that have locked its PLCs and SCADA systems, and enjoin Defendants from accessing Vaquero's computer systems. Accordingly, the relief requested is both mandatory and prohibitory in nature.

To obtain a preliminary injunction, a plaintiff "must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance

of equities tips in his favor, and that an injunction is in the public interest." Winter, 555 U.S. at 20. The Ninth Circuit determined that a party seeking a preliminary injunction "must demonstrate that it meets all four of the elements of the preliminary injunction test established in Winter." DISH Network Corp. v. FCC, 653 F.3d 771, 776 (9th Cir. 2011). The moving party carries the burden to make "a clear showing" that the Winter elements are satisfied. See Lopez v. Brewer, 680 F.3d 1068, 1072 (9th Cir. 2012) (quoting Mazurek v. Armstrong, 520 U.S. 968, 972 (1997)).

In evaluating a request for a preliminary injunction, the Court may weigh the moving party's request on a sliding-scale approach. Alliance for the Wild Rockies v. Cottrell, 632 F.3d 1127, 1135 (9th Cir. 2011). Accordingly, a stronger showing on the balance of hardships may support the issuance of a preliminary injunction where there are "serious questions on the merits … so long as the plaintiff also shows that there is a likelihood of irreparable injury and that the injunction is in the public interest." Id.; see also Global Horizons, Inc. v. U.S. Dep't of Labor, 510 F.3d 1054, 1057-58 (9th Cir. 2007) (explaining "the relationship between success on the merits and irreparable harm [is] a sliding scale in which the required degree of irreparable harm increases as the probability of success decreases," but that "a moving party must, at an 'irreducible minimum' demonstrate some chance of success on the merits").

III. Declaratory Evidence before the Court

The Ninth Circuit has determined that "[d]ue to the urgency of obtaining a preliminary injunction at a point when there has been limited factual development, the rules of evidence do not apply strictly to preliminary injunction proceedings." Herb Reed Enters. v. Fla. Entm't Mgmt., Inc., 736 F.3d 1239, 1250 n.5 (9th Cir. 2013). It is "within the discretion of the district court to accept . . . hearsay for purposes of deciding whether to issue [a] preliminary injunction." Republic of the Philippines v. Marcos, 862 F.2d 1355, 1363 (9th Cir. 1988).

Both parties have presented declaratory evidence in support of their positions.[1] The Court may consider the declarations, including any hearsay contained in them, when evaluating the request for a preliminary injunction. See Herb Reed Enters., 736 F.3d at 1250, n.5.

[1] Notably, Plaintiff did not request an evidentiary hearing to present live testimony.

A. Objections

Plaintiff objects to several statements in the declaration filed by Herda, on the grounds that they lack foundation as to personal knowledge, are conclusory in nature, or are speculation. (Doc. 26) To the extent any statement lacks foundation, it will not be considered by the Court. See Fed. R. Evid. 602 (explaining an individual may only provide testimony "if evidence is introduced sufficient to support a finding that the witness has personal knowledge of the matter"). Similarly, the Court will not give weight to argumentative statements, or statements based upon speculation. See Burch v. Regents of the Univ. of Cal., 433 F. Supp.2d 1110, 1119 (E.D. Cal. 2006) (explaining that "statements in declarations based on speculation or improper legal conclusions, or argumentative statements, are not *facts*…") To the extent the Court relies upon any statement to which Plaintiff objects, the objections are overruled.

Defendants also object to statements in the declaration of Don Lawson and its "Exhibit A". (Doc. 32). Mr. Lawson reported he "ran an application which creates a report record of the Last Login for usernames/accounts associated with the server," and "Exhibit A" is identified as "a screenshot of [his] computer including (1) the Last Login report, (2) the application as run (text), and (3) DOS window indicating that [he] accessed the control server (vaqserver1)." (Doc. 30 at 2, ¶ 2) Defendants object on the grounds of hearsay and authentication. (Doc. 32 at 1-2) However, as discussed above, the Court may consider hearsay evidence when considering a motion for a preliminary injunction. Further, Mr. Lawson reports he has personal knowledge of the control server and its ability to run a report of login information. Accordingly, Defendants' objections are overruled.

IV. Request for Judicial Notice

The Court may take notice of facts that are capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned. Fed. R. Evid. 201(b); United States v. Bernal-Obeso, 989 F.2d 331, 333 (9th Cir. 1993). Defendants request the Court take judicial notice of the "Operator Production Summary dated August 12, 2015, showing monthly production and days worked by operator, Vaquero Energy, Inc." (Doc. 23 at 1) Defendants report "the facts for which judicial notice is sought are monthly production levels reported to the California State Division of Oil, Gas, and Geothermal Resources," which are available at www.conservation.ca.gov. (Id. at 2)

The official records of the State of California, as contained in the Department of Conservation's

official website, are a source whose accuracy cannot reasonably be questioned, and judicial notice may be taken of facts on a website of a government agency. See O'Toole v. Northrop Grumman Corp., 499 F.3d 1218, 1225 (10th Cir. 2007) ("It is not uncommon for courts to take judicial notice of factual information found on the world wide web"); Denius v. Dunlap, 330 F.3d 919, 926-27 (7th Cir. 2003) (taking judicial notice of information on the website of a government agency); United States ex rel. Dingle v. BioPort Corp., 270 F.Supp.2d 968, 972 ("government documents are generally considered not to be subject to reasonable dispute . . . This includes public records and government documents available from reliable sources on the Internet"). Accordingly, the facts reported on the Department of Conservation's website are subject to judicial notice, and Defendants' request is **GRANTED**.

V. Discussion and Analysis

A. Likelihood of success on the merits

Plaintiff argues that Vaquero is likely to prevail upon its claims for violations of the Computer Fraud and Abuse act, Stored Communications Act, California's Computer Data Access and Fraud Act, and California's Unfair Competition Law. (Doc. 14 at 18-29) On the other hand, Defendants assert Plaintiffs will not succeed on these claims. (Doc. 20 at 18-25)

1. 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)

a. 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.

Here, Plaintiff contends Defendants accessed "Vaquero's Tunnell Master PLC and Ardantz Pad C PLC between May 5, 2015 and May 15, 2015, without authorization, "and deleted and modified the Passwords, ladder logic and/or data previously installed and activated on those PLC's on May 5, 2015." (Doc. 14 at 20) Further, Plaintiff asserts Defendant accessed five Steam Generators that were previously locked with a different password, as well as additional PSCs and systems. (Id.) According to Mark Creasey, an independent technician who has provided services to Vaquero since 2005, he worked with Herda as recently as May 5, 2015, "to install proper ladder logic to incorporate a minimum Firing Rate of 30% for the West Treater in the Tunnell Master PLC," and Creasey tested the ladder logic on the same date. (Doc. 14-2 at 4, Creasey Decl. ¶ 10) The same day, Herda activated alarms on

Vaquero's Ardantz Pad C PLC "from a remote access," and Creasey "personally tested and verified each alarm at the Ardantz Pad C PLC location." (Id. at 5, ¶ 11) However, on May 12, 2015, Creasey discovered that ladder logic was missing for the West Treater Control Section for the Tunnell Master PLC when a fire tube overheated and blistered, which indicated the burner was operating below the minimum firing rate of 25%-- and below the minimum set by the ladder logic he installed and tested the ladder logic with Herda on May 5, 2015. (Id.) Creasey asserts, "I did not, and could not, remove the ladder logic. The only person with access to the PLC was Jeff Herda." (Id. at 4, ¶ 10) Notably, Herda does not deny that he removed the ladder logic from the West Treater Control Section for the Tunnell Master PLC.

Further, Creasey checked the alarms for Ardantz Pad C because there had been an overflow "the night before and no alarms came in." (Id., ¶ 11) Creasey reports that when he examined the alarms, he "discovered that all alarms had been disabled in Ardantz Pad C PLC." (Id. at 5, ¶ 11) Notably, these alarms had been set with Herda on May 5, 2015 and tested by Creasey on that same date and they worked properly. *Id*. However, Creasey "did not, and could not, remove the ladder logic." *Id*. The implication, based upon who had access to the ladder logic, indicates that Herda disabled the alarms. "Without functional alarms the vessel could rupture due to high pressure injuring any person working in the immediate area and also spill contents of oil, gas and produced water onto the ground." *Id*.

On the other hand, Herda reports he "never accessed Vaquero's computers, PLCs, servers or any other devices belonging to Vaquero" after his termination.[2] (Doc. 22 at 7, ¶ 33) Despite this, Vaquero has presented evidence that ICS *did* access their server at their Edison location on May 18, 2015, ten days after the May 8, 2010 termination date. (Doc. 30 at 2 ¶ 2; Doc. 30 at 4) Though Plaintiff disputes this, Herda acknowledges that "certain PLCs were locked" and "the code on the PLCs cannot be accessed" (Id. at 4, ¶ 18), which corroborates Creasey's assertion that Herda was the only person with access to the Tunnell Master and Ardantz Pad C PLCs. (See Doc. 14-2 at 4, ¶ 10) Finally, Herda does not deny deleting the ladder logic on the Tunnell Master PLC or disabling the alarms for the Ardantz Pad C PLC.

[2] Notably, however, Herda asserts he was "terminated on or about May 8, 2015" (id. at 5, ¶ 22)—and does not deny that he accessed the systems without the knowledge of Vaquero and deleted ladder logic and deactivated the alarms before May 8.

Consequently, the evidence before the Court strongly suggests that Plaintiff will be able to demonstrate Herda accessed Vaquero's systems without permission, making changes to the Tunnell Master PLC and Ardantz Pad C PLC. There is no dispute that these systems are "protected computers" within the meaning of CFAA.

b. 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).

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, there is conflicting evidence regarding when the passwords were changed. Plaintiff contends the passwords were changed in May 2015 (Doc. 14 at 20), which would support an inference that Herda's intent was to receive payment from Vaquero. Herda reports "no passwords were changed in early May," and the passwords changed as he worked on the "logix" in the PLCs. (Doc. 22 at 6, Herda Decl. ¶ 25) Herda explains that two of the PLCs previously had a password known to Vaquero, but when he "upgraded those two PLCs" he protected the code with his passwords, beginning in 2007. (Id.) If the passwords were, in fact, changed beginning in 2007, it would be difficult for Plaintiff to establish that Herda acted with an intent to extort, as required by Section 1030(a)(7).

c. 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. To succeed on 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 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).

Here, Plaintiff contends that because of Defendants' actions, it suffered the "failure of the Wet Heater Treator controlled by the Tunnel Master PLC" and the "failure of the Vessel High Level Alarms controlled by the Ardantz Pad C PLC. (Doc. 14 at 20) In addition, Plaintiff reports that Vaquero incurred "costs associated with its attempts to recover Passwords, data and information and to assess the extent of loss or access caused by Herda and ICS. (Id., citing Doc. 14-1 at 5, Hunter Decl. ¶ 12) Specifically Mr. Hunter reports that Vaquero hired a consulting firm "to attempt to download [Vaquero's] programs fearing that Herda could, and would, remotely erase the ladder logic and instructions contained in the PLC's." (Doc. 14-1 at 5, ¶ 12) The consultant "was unable to access the programs on [the] PLC's," and Vaquero "incurred more than $12,000 in costs, fees and expenses incurred in our efforts to identify the extent of passwords, data and documents accessed and held by Herda, and attempts to fix issues related to equipment failures resulting from lack of access to computers, systems, PLC's and SCADA." (Id.)

Further, Plaintiff contends there is a threat to public health and safety because "Vaquero systems and computers include personally identifiable information and financial data of both personnel and customers" and "PLC's and SCADA control extensive and critical oil and gas production facilities

in close connection to residential and commercial areas." (Doc. 14 at 29) Mr. Hunter reports that alterations to the ladder logic, which is controlled by Defendants, could cause "a H2S gas release, high pressure steam release, fire, oil spill, or pipeline rupture." (Doc. 14-1 at 9, ¶ 21)

Finally, Plaintiff provides evidence that it must "guess at" the natural gas and oil production and sales figures that must be reported to comply with regulatory requirements. (Doc. 14-1 at 8 ¶ 20) Before the falling out with Herda, "[o]perators will read these num,bers from SCADA and enter in an Excel spreadsheet document daily that is maintained in the Edison server. [However,] [s]ome PLC's that contain this data are not accessible due to password blocking." *Id.* As a result, "these numbers are not being reported accurately." *Id.* Thus, Plaintiff has submitted evidence sufficient to show damages under the CFAA, as defined by18 U.S.C. § 1030(e)(8), and as required to pursue a private action under 18 U.S.C. § 1030(g).

While Herda counters this evidence with his claims that each of the pieces of equipment can be shut down manually by being personally present at the site of the affected equipment (Doc. 22 at 7 ¶ 31), he fails to provide any information that this can occur within the timeframe necessary to avoid mass damage. Likewise, he fails to demonstrate any foundation for his explanation of the ability to shut the equipment down. Finally, he fails to explain how the production and sales figures on the password-protected PLCs may be accessed such to obtain the correct figures. Based upon the foregoing, the Court finds Plaintiff has demonstrated a likelihood of success on the merits for a claim arising under Section 1030(a)(5).

2. Violation of Cal. Pen. Code § 502

The California Computer Data Access and Fraud Act "expand[s] the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a). Here, Plaintiff asserts Defendants violated Section 502(c)(5), which imposes liability upon an individual who:

> Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

Cal. Penal Code § 502(c)(5). The California Computer Data Access and Fraud Act also authorizes the

owner of the computer, network, system, program or data "who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) [to] bring a civil action against the violator for compensatory damages and injunctive relief or equitable relief." Id., § 502(e)(1).

Defendants assert "Vaquero is not likely to prevail on its claim for a violation of Penal Code," because "[n]o evidence has been provided showing that business operations have been disrupted, or that access to any computer service has been denied." (Doc. 20 at 8-9) Further, Defendants contend that "Vaquero is still using its computers unhindered, and is still operating its SCADA system." (Id. at 9) In support of these assertions, Defendants observe that "Vaquero's mineral production increased from April 2015 to May 2015, with Vaquero producing more than 60,000 barrels of oil in May 2015, as opposed to approximately 58,000 barrels in April." (Id.)

Plaintiff does not dispute the production numbers identified by Defendants, but argues its business operations have been disrupted because "the equipment and PLC's did NOT operate as planned" when "a heater fire tube overheated and blistered" and "a test vessel over-flowed." (Doc. 24 at 6) In addition, the evidence before the Court demonstrates that the Vaquero employees were entitled to access to the information stored on its PLCs because they were aware of the passwords prior to changes made when Herda "updated" the code. (See Doc. 14-1, Hunter Decl. ¶¶ 10-11; Doc. 22 at 4 and, Herda Decl. ¶¶ 16, 25) From this, the Court may conclude the Vaquero employees were "authorized users" as required under Cal. Penal Code § 502. Thus, Plaintiff has presented evidence that Defendants have caused the denial of computer services to authorized users of the PLCs through locking the ladder logic and not producing the information requested by Vaquero.

Furthermore, the evidence before the Court indicates that the passwords to the logic were imposed without the permission of Vaquero. Although Herda asserts that "Mr. Hunter never expressed to [him] that he cared about the PLCs and whether they were password-protected" (Doc. 22 at 7, ¶ 29), at the hearing, his counsel admitted he never sought permission to do so and Vaquero never granted permission. He also admits that Vaquero employees requested information including "documentation and programs" related to the PLCs on several occasions beginning in March 2015. (See id. at ¶¶ 28-30) Likewise, he admits that Hunter "would not have knowledge of passwords" which indicates that there was never any agreement that Plaintiff agreed that passwords could be imposed on the PLCs.

Also, as discussed above, Herda acknowledges that Vaquero knew the passwords to its PLCs before he started working with the company. (Id., ¶ 25) There is no evidence that placing passwords on the code—and thereby restricting Vaquero from its own PLCs—was an act taken with the permission of Vaquero. Thus, it is likely that Plaintiff will succeed on the merits of this claim because the imposition of the passwords was without the permission of Vaquero, and caused the denial of access to previously authorized users of its systems.

3. 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).

For example, 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) rev'd sub nom. In re Pharmatrak, 329 F.3d 9 (1st Cir. 2003) (emphasis added), the Court held,

> 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**.

Here, though Plaintiff alleges Defendants exceeded the scope of the authorization given to access the PLCs and SCADA systems, they have failed to convince the Court that they are "facilities" under the SCA. Thus, the Court concludes that Plaintiffs have not demonstrated a likelihood of success on the merits of this claim.

4. Unfair Competition Law, Cal. Bus. & Prof. Code § 17200

California's Unfair Competition Law prohibits any "unlawful, unfair, or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200. Accordingly, there are three prongs under which a claim may be established under §17200. Daro v. Superior Court, 151 Cal.App.4th 1079, 1093 (2007) ("Because section 17200 is written in the disjunctive, a business act or practice need only meet one of the three criteria—unlawful, unfair, *or* fraudulent—to be considered unfair competition"); Lozano v. AT&T Wireless Servs., 504 F.3d 718, 731 (9th Cir. 2007) ("[e]ach prong . . . is a separate and distinct theory of liability"). Further, a claim under Section 17200 must rest on a violation of another law. Farmers Ins. Exch. v. Superior Court, 2 Cal.4th 377, 383 (1992).

Here, it is unclear under what prong(s) Plaintiff seeks to proceed under for this claim. However,

actions prohibited by Section 17200 include "any practices forbidden by law, be it civil or criminal, federal, state, or municipal, statutory, regulatory, or court-made." Saunders v. Superior Court, 27 Cal.App.4th 832, 838-39 (1994). As explained above, Plaintiff demonstrates a likelihood of success on the merits claims for violations of the Computer Fraud and Abuse Act and California's Computer Data Access and Fraud Act. Thus, it appears Plaintiff has also demonstrates a likelihood of success on the merits for this cause of action. See Saunders, 27 Cal.App.4th at 838-39.

B. Irreparable Harm

The propriety of a request for injunctive relief hinges on a significant threat of imminent irreparable harm. Caribbean Marine Serv. Co. v. Baldridge, 844 F.2d 668, 674 (9th Cir. 1988). Thus, a plaintiff must demonstrate an immediate irreparable harm as a prerequisite to preliminary injunctive relief. Los Angeles Memorial Coliseum Com. v. Nat'l Football League, 634 F.2d 1197, 1201 (9th Cir. 1980). A speculative injury is not sufficient support the issuance of a preliminary injunction. Goldie's Bookstore, Inc. v. Superior Court, 739 F.2d 466, 472 (9th Cir. 1984).

Plaintiff contends that Vaquero would suffer irreparable harm if the request for a preliminary injunction is denied for the following reasons:

> (1) Herda and ICS refuse to deliver Passwords to Vaquero, (2) the Passwords control access to Vaquero systems, computers, PLC's and SCADA, (3) Vaquero systems and computers include personally identifiable information and financial data of both personnel and customers; (4) PLC's and SCADA control extensive and critical oil and gas production facilities in close connection to residential and commercial areas; (5) Herda and ICS has recently accessed Vaquero PLC's to delete and modify ladder logic and alarms; and (6) Herda and ICS has the present ability to delete or modify virtually any computer, system, PLC or SCADA causing a complete and catastrophic failure to each and every oil and gas production field and equipment as well as Vaquero's financial, personnel, customer and regulatory data and information.

(Doc. 14 at 29) According to Plaintiff, "Since Herda and ICS control Vaquero's Passwords –thereby its systems, computers, PLC's and SCADA, Vaquero will not be able to control the security of personal information or financial data." (Id. at 31) In addition, Plaintiff contends there is a threat of irreparable harm to "Vaquero personnel, residents and nearby businesses" due to failures of its systems and equipment, and the inability to access the PLCs to cure any errors. (Doc. 14 at 32, citing Creasey Decl. ¶ 10, Hunter Decl. ¶ 18) Mr. Hunter reports that the failure of the West Heater Treater PLC could have "caused the crude oil and natural gas inside the pressurized vessel to ignite and explode," and "there are

5-10 Vaquero employees and contractors working within 100' of this equipment at any given time during daylight hours, 7 days a week." (Doc. 14-1 at 6, ¶ 18) Similarly, Mr. Creasey reports the failure could have "caused the crude oil and natural gas inside the pressurized vessel to enter into the Combustion section of the Firetube at [which] point the unit would ignite and explode." (Doc. 14-2 at 4, ¶ 10) Although he was able to fix the problem, Creasey asserts this was only a temporary solution—and one that cannot be used on other equipment. (Id.)

Further, Plaintiff reports that after this motion was filed, Vaquero "again experienced a process failure in the master Tunnell PLC at 1:12am on Tuesday, July 28, 2015 that caused the East Heater Treater to overflow out of the gas phase piping." (Doc. 24-2 at 2, Creasey Decl. ¶ 2) Creasey reports that "[o]il flowed out of the gas piping and into the casing vapor recovery compressors," which "caused the south CVR compressor to seize." (Id.) According to Creasey, "The cause of the PLC failure is unknown since [Vaquero] can't access the PLC to see what the problem was – and is." (Id.) Therefore, Plaintiff asserts there remains a high risk of imminent harm exacerbated by the inability of Vaquero to check its PLCs and the ladder logic directing the equipment.

Defendants question whether Vaquero would continue to operate its fields "if [it] cannot prevent catastrophic personal injury and environmental damage due to its inability to monitor and control its operations." (Doc. 20 at 19) Defendants contend, "it is the end devices that likely fail," rather than the "computers, networks, SCADA, PLCs, or any other type of computer system." (Id.; see also Doc. 22 at 7, Herda Decl. ¶ 31) Herda argues that the end devices "can be manually powered down in the event of any malfunction" and "can also be operate pneumatically." (Id., ¶ 31) Further, Defendants contend that "if Vaquero were to shut down its field operations, the damage would be monetary." (Doc. 20 at 20) Therefore, Defendants contend Plaintiff is unable to show an imminent risk of irreparable harm.

Notably, however, the failure of the West Heater Treater, which was controlled by the Tunnel Master PLC, was not due to the failure of an "end device," but rather was caused by the missing ladder logic which should have been contained on the PLC. Further, Vaquero maintains that "review of ladder logic and modification of data, triggers and levels connected to such ladder logic is necessary to address an unplanned incident or malfunction of any piece of equipment." (Doc. 24 at 14) Thus,

Vaquero is unable to predict similar malfunctions through the review of the data stored on the PLCs and SCADA systems. Notably, Herda admits that a "significant power malfunction" would interrupt the operation of the PLC which, it appears, could cause great damage to the environment, people and equipment. The Supreme Court observed that "environmental injury, by its nature, can seldom be adequately remedied by money damages and is often permanent or at least of long duration, i.e., irreparable." See Amoco Prod. Co. v. Village of Gambell, 480 U.S. 531, 545 (1987). Consequently, the Ninth Circuit has determined that, "when environmental injury is 'sufficiently likely, the balance of harms will usually favor the issuance of an injunction to protect the environment.'" Sierra Club v. United States Forest Service, 843 F.2d 1190, 1195 (9th Cir. 1988) (quoting Amoco, 480 U.S. at 545).

Given Vaquero's inability to check the ladder logic on its systems and the risks of equipment failures—and the potential events related thereto— and the failure of the Tunnell Master PLC on two occasions since the termination of the relationship with Plaintiff, the Court finds Plaintiff carries its burden to identify an imminent risk irreparable harm, and this factor weighs in favor of the issuance of a preliminary injunction.

C. Balancing of Equities

Defendants contend that "ICS would suffer irreparable injury if an injunction were granted" because "ICS authored the code, and the code is proprietary and afforded protection by copyright laws." (Doc. 20 at 20-21, emphasis omitted) Defendants explain: "Any order forcing ICS to provide its passwords to the code will result in Vaquero's unfettered and unauthorized use of ICS's proprietary, confidential, and private material without remuneration to ICS. Moreover, it would subject ICS's proprietary information and intellectual property to use by the general public, including ICS's competitors." (Id. at 21) According to Defendants, if ICS's competitors are able to obtain the code, "they would gain the unfair advantage of utilizing the same code with less time, effort, and energy." (Id.)

On the other hand, Plaintiff argues "the ladder logic fails as proper subject matter of copyright – along with passwords, data and materials (physical embodiments of the alleged work." (Doc. 14 at 33) Plaintiff contends that to the extent the code is subject to copyright protections, the proper owner of the code is Vaquero, because: "(1) all instructions, structure and logic was provided to Herda and ICS by

Vaquero employees and representatives, (2) all initial ladder logic and significant portions of the current ladder logic were NOT created by Herda and ICS, (3) the actions by Herda and ICS amount to merely clicking a drop-down menu of options under the Rockwell Automation software in accord with Vaquero instructions and (4) passwords and data are not copyrightable works." (Id. at 35)

Importantly, however, the Court need to resolve the issue of whether the code, ladder logic, and related data/information is subject to copyright at this juncture. To the extent that Defendants are concerned about the copying of the code, the Court can prohibit Plaintiff from replicating the codes or offering access to ICS' competitors. Given the potential harms and equipment failures—which put Vaquero employees and the public at risk—the Court finds Plaintiff carried its burden to show the balance of equities tips in its favor. Consequently, this factor weighs in favor of the issuance of a preliminary injunction.

D. Public Interest

As Defendants observe, "it is virtually axiomatic that the public interest can only be served by upholding copyright protections and correspondingly, preventing the misappropriation of skills, creative energies, and resources which are invested in the protected work." (Doc. 20 at 21, quoting Warner Bros. Entertainment Inc. v. WTV Systems, Inc., 824 F.Supp.2d 1003, 1015 (C.D. Cal. 2011)).

On the other hand, as discussed above, there is a risk of injuries to the environment and the public due to missing ladder logic and equipment malfunctions. According to Mr. Hunter, the West Heater Treater PLC is "located .3 miles from the nearest home," and "H2S gas (hydrogen sulfide) is present and associated with the production of the crude oil which is poisonous." (Doc. 14-1 at 6-7, Hunter Decl. ¶ 18) Thus, the public would not be served if the Court declined to issue a preliminary injunction.

E. Posting of a Bond

Pursuant to Fed. R. Civ. P. 65(c), "[t]he court may issue a preliminary injunction or a temporary restraining order only if the movant gives security in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained." However, "[t]he court has discretion to dispense with the security requirement, or to request mere nominal security, where requiring security would effectively deny access to judicial review." California

ex rel. Van De Kamp v. Tahoe Regional Planning Agency, 766 F.2d 1319, 1325 (9th Cir. 1985), *amended on other grounds*, 775 F.2d 998 (9th Cir. 1985).

Here, Plaintiff has not presented any evidence that posting a bond would impose a financial burden upon the company. Further, Defendants would suffer financial loss if the injunction is granted and they are later able to show the codes are subject to copyright protection such to provide them a proprietary interest. At the hearing, Defendants indicated the value of the interest was $100,000 per year—and noted Defendants previously billed Plaintiff approximately $50,000 per month for services. Accordingly, the Court finds the estimate of $100,000 per year is a reasonable request for a bond. Given the anticipated length of the action, Plaintiff shall post a bond of $200,000.

VI. Conclusion and Order

Based upon the foregoing, Plaintiff has carried the burden to demonstrate Vaquero is likely to succeed on the merits of several claims, likely to suffer irreparable harm without the issuance of an injunction, that the balance of equities tip in their favor, and the requested relief is in the public interest. See Winter, 555 U.S. at 20; Lopez, 680 F.3d at 1072.

Accordingly, **IT IS HEREBY ORDERED**:

1. Plaintiff's motion for a preliminary injunction is **GRANTED**, subject to Plaintiff posting a $200,000 bond with the Clerk of Court by the close of business on Friday, September 4, 2015;
2. Defendants and their agents, representatives, and persons acting in concert therewith are enjoined and restrained from:
    a. accessing Vaquero's computers, servers, and/or firmware and related attached equipment and components (including, without limitation, programmable logic controllers ("PLC"s) and supervisory control and data acquisition ("SCADA") systems;
    b. preventing Vaquero's access to, and unrestricted use of, Vaquero's computers, servers, and/or firmware and related attached equipment and components (including, without limitation, PLCs and SCADA systems; and
    c. viewing, deleting, copying, disposing of, destroying, transferring to third parties,

or altering in any way any system structure, data, documents, software, files and/or folders (including, without limitation, so-called "ladder logic") that Herda and/or ICS downloaded, otherwise copied, or in any way received from Vaquero during or after Herda and/or ICS's performance or services to Vaquero;

3. Upon presentation of proof of Defendant posting the bond ordered herein, Defendants **SHALL** immediately return to Vaquero any and all system structure, data, documents, software, files and/or folders that Herda and/or ICS downloaded, otherwise copied, or in any way received from Vaquero during or after Herda and/or ICS's performance or services to Vaquero including, without limitation:

   a. passwords, user-names, .dat files, and all related access controls for all Vaquero computers, servers, and/or firmware and related attached equipment and components (including, without limitation, PLCs and SCADA systems;

   b. documentation of all software development, programming and firmware instructions (including so-called ladder logic);

   c. source code and object code for all software development, programming and firmware instructions (including so-called ladder logic); and

4. The Order becomes effective immediately after the bond is posted and continues until the Court enters a final judgment in this action or otherwise lifts the injunction.

IT IS SO ORDERED.

Dated: **August 28, 2015**

/s/ Jennifer L. Thurston
UNITED STATES MAGISTRATE JUDGE