1

2

3

4

5

6   UNITED STATES DISTRICT COURT

7   DISTRICT OF NEVADA

8   * * *

9 ORACLE USA, INC., a Colorado corporation;)
ORACLE AMERICA, INC., a Delaware)
10 corporation; and ORACLE)   2:10-CV-00106-LRH-PAL
INTERNATIONAL CORPORATION, a)
11 California corporation;)
)   <u>ORDER</u>
12   Plaintiffs,)
)
13 v.)
)
14 RIMINI STREET, INC., a Nevada)
corporation; and SETH RAVIN, an individual;)
15   )
               Defendants.)
16   )

17   Before the court is defendants Rimini Street, Inc. ("Rimini") and Seth Ravin's ("Ravin")

18 (collectively "defendants") renewed motion for judgment as a matter of law. ECF No. 913.

19 Plaintiffs Oracle USA, Inc.; Oracle America, Inc.; and Oracle International Corporation

20 (collectively "Oracle") filed an opposition (ECF No. 957) to which defendants replied

21 (ECF No. 976).

22 **I.   Facts and Procedural History**

23   This action has an extensive factual and procedural history.[1] In brief, plaintiff Oracle

24 develops, manufacturers, and licenses computer software. Oracle also provides support services to

25 ———————————————

26   [1] For a more in depth examination of the factual and procedural history of this action, see the court's order regarding the parties' motions for summary judgment. *See* ECF Nos. 474, 476.

customers who license its software. Defendant Rimini is a company that provides similar software support services to customers licensing Oracle's software and competes directly with Oracle to provide these services. Defendant Ravin is the owner and CEO of defendant Rimini.

On January 25, 2010, Oracle filed a complaint for copyright infringement against defendants alleging that Rimini copied several of Oracle's copyright-protected software programs onto its own computer systems in order to provide software support services to customers. ECF No. 1. In June 2011, Oracle filed a second amended complaint alleging thirteen causes of action against Rimini: (1) copyright infringement; (2) violation of the Federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §§ 1030(a)(2)(C), (a)(4), & (a)(5); (3) violation of the California Computer Data Access and Fraud Act, Cal. Penal Code § 502; (4) violation of the Nevada Computer Crimes Law, NRS § 205.4765; (5) breach of contract; (6) inducement of breach of contract; (7) intentional interference with prospective economic advantage; (8) negligent interference with prospective economic advantage; (9) unfair competition; (10) trespass to chattels; (11) unjust enrichment; (12) unfair practices; and (13) accounting. ECF No. 146.

A jury trial was held on Oracle's claims from September 14, 2015, through October 13, 2015. On October 13, 2015, the jury returned a verdict on Oracle's claims and found that defendant Rimini engaged in copyright infringement of Oracle's copyrighted PeopleSoft, J.D. Edwards, and Siebel-branded Enterprise Software products. ECF No. 896. The jury also found that both defendant Rimini and Ravin violated the California Computer Data Access and Fraud Act ("CDAFA") and the Nevada Computer Crimes Law ("NCCL"). *Id*. After the jury verdict, defendants filed the present Rule 50(b) motion for judgment as a matter of law on the CDAFA and NCCL claims. ECF No. 913.

II.   Legal Standard

Under Rule 50(b), after the court enters judgment, a party may file a renewed motion for judgment as a matter of law. Rule 50 provides that judgment as a matter of law is appropriate if "a reasonable jury would not have a legally sufficient evidentiary basis to find for the party on that

issue." FED. R. CIV. P. 50(a)(1). In other words, Rule 50 "allows the trial court to remove cases or issues from the jury's consideration when the facts are sufficiently clear that the law requires a particular result." *Weisgram v. Marley Co.*, 528 U.S. 440, 448 (2000).

Under Rule 50, the court reviews whether "substantial evidence" supports the jury verdict. *See Hagen v. City of Eugene*, 736 F.3d 1251, 1256 (9th Cir. 2013). "A jury's verdict *must* be upheld if it is supported by substantial evidence, which is evidence adequate to support the jury's conclusion, even if it is also possible to draw a contrary conclusion." *Pavao v. Pagay*, 307 F.3d 915, 918 (9th Cir. 2002) (emphasis added). A verdict is not supported by substantial evidence "when the evidence, construed in the light most favorable to the nonmoving party, permits only one reasonable conclusion, which is contrary to the jury's verdict." *Hagen*, 736 F.3d at 1256. In reviewing a Rule 50 motion, the court "must disregard evidence favorable to the moving party that the jury is not required to believe," "must view the evidence in the light most favorable to the nonmoving party," and must "draw all reasonable inferences in [the non-moving] party's favor." *Pavao*, 307 F.3d at 918.

III.   Discussion

In their present Rule 50(b) motion, defendants argue that the jury's findings of liability on the CDAFA and NCCL claims are unsupported by the evidence at trial and invalid as a matter of law. *See* ECF No. 913. In particular, defendants raise five separate challenges to the jury's verdict on the CDAFA and NCCL claims. First, defendants contend that neither California nor Nevada's computer access statute applies in this action under general choice-of-law principles. Second, defendants argue that plaintiff Oracle International Corporation ("OIC") lacked standing to allege a claim under either statute, and as such, the court must set aside both the jury's verdict and the $5.6 million in damages the jury awarded to OIC under both statutes. Third, defendants argue that their conduct, as established by the evidence at trial, did not violate either statute as a matter of law. Fourth, defendants contend that Oracle is not entitled to recover economic damages, including lost profits damages, under either statute. Finally, defendants argue that both the CDAFA and the

3

NCCL are facially unconstitutional and unconstitutional as applied in this action. The court shall address each challenge below.

A. Facts Relevant to the Computer Law Claims

Plaintiff Oracle America, Inc. ("Oracle America") owns and operates a website that operates as an online database for Oracle's software customers. This database contains millions of technical support files for Oracle's copyrighted Enterprise Software programs, including its PeopleSoft, J.D. Edwards, and Siebel branded software. During the relevant time period of the CDAFA and NCCL claims - late 2006 through early 2009 - this online database was accessible through a website that required both the customer's unique login identification[2] ("login") and acceptance of the website's specific Terms of Use.

Oracle America's online database did not have a built-in mechanism to allow Oracle's software customers to download large numbers of files at one time; rather, Oracle's customers had to individually search for, identify, and download any files and/or documentation that they desired from the vast catalog of available files. With hundreds of thousands, or even millions, of files available for each software product, this could be a time consuming process if the licensee required extensive support files to use the licensed Enterprise Software. Recognizing the need for customers to quickly find and download desired files, Oracle America encouraged its customers to use automated downloading tools as a means to obtain the requested files in a timely manner. During the time from early 2006 until February 2007, defendant Rimini accessed Oracle America's website using a client's unique login and used permitted automated downloading tools to download technical files for that client's software from the Oracle America website onto its own computer systems and servers.

///

---

[2] As part of a customer's software license agreement with Oracle, the customer was entitled to download files from the website related to the licensed software - including instruction manuals, regulatory updates, and other modification files. In order to access the website, each customer was given a unique account and password to log into the website as part of their software license agreement.

On February 19, 2007, in response to an increased volume of mass downloads through the use of automated tools, and other server and database pressures, Oracle America changed its website's Terms of Use to specifically prohibit the use of "any software routines commonly known as robots, spiders, scrapers, or any other automated means to access [the site] or any other Oracle accounts, systems or networks." This change in the Terms of Use prohibited the use of previously allowed automated downloading tools. Defendants knew of the change to the Terms of Use and quit using automated tools to download files from the website at that time.

In November 2008 through January 2009, more than a year after Oracle America changed its Terms of Use, defendant Rimini began reusing automated tools on the website in violation of the Terms of Use (terms which it had to specifically agree to when logging on to the website) in order to download full libraries of support documents and files for entire software products lines - each involving hundreds of thousands of different files - in an attempt to have a complete catalog of all of the technical files that were available on the website at that time. Rimini downloaded these technical and support files directly on to its own computer systems, thereby allowing it to more easily service Oracle software for its clients and compete directly with Oracle for software support services. In all, more than a million attempts to download files from the website were conducted by Rimini in that three month period.

Oracle investigated the increased traffic and downloading on the website and discovered Rimini's use of automated downloading tools. After discovering Rimini's conduct, Oracle America notified Rimini that its conduct was in violation of the website's Terms of Use and blocked Rimini's IP address preventing it from accessing the website. Rimini then obtained additional IP addresses so that it could continue to download files from the website despite continued warnings and action by Oracle America including blocking several of the new IP addresses. Rimini's near constant access to the website and continuous downloading caused slow-downs and server interruptions, preventing Oracle customers from obtaining files from the website. These slow-downs eventually led to a several hour shutdown of the website which required the database

servers housing the technical and support files to be restarted before any other Oracle customers could access the website. After January 2009, and having obtained millions of technical and support files from the website, Rimini stopped using automated tools to download files from Oracle America's website.

B. Computer Law Claims

As part of this lawsuit, plaintiff Oracle brought claims against defendants under both the CDAFA and the NCCL. *See* ECF No. 146. The CDAFA provides in relevant part that any person who "[k]nowingly accesses and without authorization 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" or "[k]nowingly and without permission uses or causes to be used computer services" is guilty of a public offense. CAL. PENAL CODE §502(c)(2)-(3). Pursuant to the CDAFA, a private party who is "the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." CAL. PENAL CODE §502(e)(1).

Similarly, the NCCL provides that "a person who knowingly, willfully and without authorization: (a) Modifies; (b) Damages; (c) Destroys; (d) Discloses; (e) Uses; (f) Transfers; (g) Conceals; (h) Takes; (i) Retains Possession of; (j) Copies; (k) Obtains or attempts to obtain access to, permit access to or causes to be accessed; or (l) Enters . . . data, a program or any supporting documents which exist inside or outside a computer, system or network" or " who knowingly, willfully and without authorization: (a) Destroys; (b) Damages; (c) Takes; (d) Alters; (e) Transfers; (f) Discloses; (g) Conceals; (h) Copies; (i) Uses; (j) Retains possession of; or

(k) Obtains or attempts to obtain access to, permits access to or causes to be accessed . . . a computer, system or network" is guilty of a misdemeanor. NRS §§205.4761(1) & (3). Under the NCCL, "any victim of a crime described in [NRS §205.4761] may bring a civil action to recover: (a) Damages for any response costs, loss or injury suffered as a result of the crime; (b) Punitive Damages; and (c) Costs and reasonable attorney's fees incurred in bringing the civil action." NRS §205.511(1).

After a four week jury trial and several days of deliberation, the jury returned a verdict in favor of plaintiffs Oracle America and OIC and against defendants Rimini and Ravin on both state computer law claims. ECF No. 896. In the verdict, the jury awarded Oracle America damages in the amount of $8,827,000 and OIC damages in the amount of $5,600,000 under the CDAFA. The jury also awarded Oracle America damages in the amount of $8,827,000 and OIC damages in the amount of $5,600,000 under the NCCL. Thereafter, defendants filed the present Rule 50(b) motion. ECF No. 913.

C. Choice-of-Law Challenges

Initially, defendants raise three separate "choice-of-law" challenges to the jury's verdict under general choice-of-law principles, the Commerce Clause, and the extraterritoriality doctrine. *See* ECF No. 913. In these challenges, defendants argue that the jury should not have been allowed to reach a verdict on either the CDAFA or NCCL claims because Oracle failed to introduce into evidence any predicate facts identifying where the alleged violating conduct occurred or where Oracle America's affected servers were located. Without this evidence, defendants contend there was no basis for the jury to conclude that either the California or Nevada statute applied to defendants' conduct.

The court has reviewed the documents and pleadings on file in this matter and finds that defendants' choice-of-law challenges are without merit. "A Rule 50(b) motion for judgment as a matter of law is not a freestanding motion. Rather, it is a renewed Rule 50(a) motion." *E.E.O.C. v. Go Daddy Software, Inc.*, 581 F.3d 951, 961 (9th Cir. 2010). As such, a Rule 50(b) motion is

limited to the grounds asserted in the pre-deliberation Rule 50(a) motion, and a party cannot "raise

arguments in its post-trial motion for judgment as a matter of law under Rule 50(b) that it did not

raise in its preverdict Rule 50(a) motion." *Freund v. Nycomed Amersham*, 347 F.3d 752, 761 (9th

Cir. 2003); *see also, Murphy v. City of Long Beach*, 914 F.2d 183, 186 (9th Cir. 1990) (judgment

notwithstanding the verdict is "improper if based upon grounds not alleged in a directed verdict"

motion). Here, defendants failed to raise these challenges in their initial Rule 50(a) motion, and as

such, they are precluded from raising these challenges in the present Rule 50(b) motion. Therefore,

the court shall deny defendants' motion as to these challenges.

D. Lack of Standing

Defendants' second challenge to the jury verdict is that plaintiff OIC lacked standing to

bring a claim under either the CDAFA or NCCL because Oracle failed to present any evidence at

trial that OIC was either (1) the "owner or lessee" of the computer system accessed by defendants

as required under the CDAFA, or (2) was the "victim" of any unauthorized access by defendants

as required under the NCCL. *See* ECF No. 913. Accordingly, defendants argue that the jury's

verdict awarding $5.6 million to OIC under both the CDAFA and the NCCL must be set aside. The

court disagrees.

Initially, the court notes that defendants failed to properly raise this argument in their

Rule 50(a) motion.[3] Therefore, this challenge fails as a matter of law. *See Freund*, 347 F.3d at 761.

However, even if defendants had properly raised this argument in their Rule 50(a) motion,

defendants' standing challenge is without merit. Defendants argue that only the "owner or lessee"

---

[3] In their reply to the present Rule 50(b) motion, defendants direct the court to a one-sentence footnote
in their initial Rule 50(a) motion to support the proposition that they properly raised this argument prior to the
jury verdict. In that footnote, while arguing that Rimini did not breach any contract with Oracle, defendants
stated that "[OIC] failed to prove it even had computer systems." *See* ECF No. 865, p.13 n.3. Defendants now
claim that this one-sentence footnote constituted a fully fleshed out argument that OIC lacked standing to bring
a claim under either the CDAFA and NCCL. The court disagrees, and finds that this single sentence is
insufficient to properly raise the issue in defendants' Rule 50(a) motion. The footnote in question did not refer
to OIC's standing to assert any claim, particularly claims brought under the CDAFA and the NCCL. Rather,
the footnote only concerned the availability of Oracle's separately pled breach of contract claim.

of a computer has standing to bring a claim under the CDAFA. However, the CDAFA provides that "the owner or lessee of the computer, computer system, computer network, computer program, *or data* who suffers damage . . . may bring a civil action against the violator[.]" CAL. PENAL CODE §502(e)(1) (emphasis added). The NCCL has similar language related to the ownership of data. *See* NRS §205.4761(1). The evidence at trial sufficiently established OIC's interest and ownership of the technical files and support materials that were downloaded by defendants. Thus, the evidence established unequivocally that OIC had standing to allege a claim under both the CDAFA and the NCCL. Therefore, the court shall deny defendants' standing challenge.

E. Defendants' Conduct

As addressed in subsection B, the CDAFA and NCCL prohibit the unauthorized access of a computer system. *See* CAL. PENAL CODE § 502(c); NRS § 205.4761. As both the CDAFA and NCCL are criminal statutes that authorize civil claims, the court must construe the statutes strictly in determining whether either statute prohibits defendants' conduct. *See e.g., LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1134-35 (9th Cir. 2009); *United States v. Nosal*, 642 F.3d 781, 863 (9th Cir. 2011). However, as the CDAFA and NCCL use the term "knowingly" in describing the proscribed conduct, there is no requirement that the jury find that defendants acted with the specific intent to violate either statute when they used, or caused to be used, automated downloading tools on Oracle America's website. *See The People v. Hawkins*, 98 Cal. App. 4th 1428, 1438 (Cal. App. 2002) ("A requirement of knowledge is not a requirement that the act be done with any specific intent . . . the word 'knowing' as used in a criminal statute imports only an awareness of the facts which bring the proscribed act within the terms of the statute.").

At trial, Oracle proffered evidence that defendants' violated the Terms of Use of Oracle America's website when Rimini used, and defendant Ravin caused to be used, automated downloading tools to download vast quantities of files from the website. Defendants argue that neither statute specifically prohibits the use of automated downloading tools or in any way penalizes the means of accessing information on a computer, and therefore, their conduct did not

9

violate either statute as a matter of law. *See* ECF No. 913. Further, defendants argue that the undisputed evidence at trial established that they had permission and authorization from their clients to access Oracle America's website using the clients' unique login to obtain support materials on their clients' behalf. *Id*. The court disagrees.

As to defendants' first argument, defendants contend that nothing in the plain language of either statute prohibits the use of automated downloading tools when accessing or using a computer system. However, the CDAFA is not limited to "using" a computer. In fact, the CDAFA specifically covers the knowing, unauthorized "taking" and "copying" of data. CAL. PENAL CODE § 502(c)(2). In *United States v. Christensen*, the Ninth Circuit expressly held that simply "logging into a database with a valid password and subsequently taking, copying, or using the information in the database improperly" constitutes a violation of the CDAFA. *United States v. Christensen*, 801 F.3d 970, 994 (9th Cir. 2015).

Here, the evidence at trial established that defendants' activity on the database website during the relevant time period from November 2008 through January 2009 exceeded all of Oracle's other customers combined. Further, the evidence established that defendants used, or caused to be used, automated downloading tools on the website after specifically agreeing not to use such tools by accepting the website's Terms of Use prior to accessing the online database of technical and support files. Using automated downloading tools in violation of Oracle America's website's Terms of Use allowed defendants to take and copy millions of files from the website onto their own computer systems where they were then able to duplicate and modify the files to service their clients. Defendants accomplished this downloading despite Oracle's efforts to block Rimini's IP addresses and prevent Rimini, who was not an Oracle customer and did not have its own unique login, from accessing the website. Defendants do not contest that they knowingly accessed the website. Nor do defendants contest that they took and subsequently used data from the website in a manner that was prohibited by the website's Terms of Use. Taking all of this evidence together in the light most favorable to Oracle as the non-moving party, the evidence at trial was

1   sufficient to support the jury's finding that defendants took the data in a manner that was

2   prohibited by the website's Terms of Use.

3   　　　　As to defendants' second argument, defendants argue that the testimony and documents at

4   trial established that Rimini was specifically authorized by its clients (who had software licenses

5   for Oracle software) to access Oracle America's website. Defendants contend that it is undisputed

6   that they had permission from their clients to access the website in order to download support

7   materials for those clients and that defendants did not exceed the scope of that authorization.

8   Therefore, because they had authority to access the website, defendants argue that the jury verdict

9   is not supported by the evidence.

10   　　　　Defendants' argument is without merit. First, defendants' contention that the key inquiry

11   under the CDAFA and the NCCL is whether or not they had authority to access the website is

12   misplaced. "[The CDAFA] does not require *unauthorized* access [of a computer system.] It merely

13   requires *knowing* access . . . ." *Christensen*, 801 F.3d at 993. Therefore, defendants' claim that they

14   had permission from their clients to access Oracle America's website is irrelevant. What makes a

15   defendant's access of a computer system unlawful is that the person "without permission takes,

16   copies, or makes uses of" data on the computer. CAL. PENAL CODE § 502(c)(2); *see also,*

17   *Christensen*, 801 F.3d at 993 (stating that a plain reading of the CDAFA "demonstrates that its

18   focus is on unauthorized taking or use of information). In *Christensen*, the court held that liability

19   is established under the CDAFA where a defendant logs into a website or database "with a valid

20   password and subsequently, [takes, copies, or uses] the information in the database improperly."

21   801 F.3d at 994. And while the case law on the NCCL is limited, the statute covers the same

22   conduct as the CDAFA and the same legal reasoning should apply. *See* NRS §§205.4761(1) & (3).

23   　　　　Second, the evidence at trial established that defendants knew they were not permitted to

24   use automated tools to download files from Oracle America's website, but did so regardless of the

25   specific prohibition against such tools in the website's Terms of Use. Further, the evidence

26   established that defendants took affirmative technical measures to evade Oracle's detection and

circumvent Oracle's efforts to block them from accessing the website by obtaining additional IP addresses after being blocked from the website. Thus, there was sufficient evidence to support the jury's verdict that defendants "knowingly accessed and *without permission* took or made use of any data" from the website. *See* ECF No. 888, JI No. 47.

The jury instructions on both the CDAFA claim and the NCCL claim further support the jury's liability verdict because the jury instructions specifically required the jury to find that defendants either did not have authorization to take files from Oracle America's website or that defendants exceeded whatever authorization that they believed they had. *See* ECF No. 888, JI No. 47, ("If you find that Rimini Street and/or Seth Ravin believed it had authorization to access Oracle America's and/or Oracle International Corporation's computer, and did not exceed that authorized access, then you must find that Rimini Street and/or Seth Ravin did not violate the California Computer Data Access and Fraud Act."); *see also*, JI No. 53 ("If you find that Rimini Street and/or Seth Ravin believed it had authorization to access Oracle America's and/or Oracle International Corporation's computer, and did not exceed that authorized access, then you must find that Rimini Street and/or Seth Ravin did not violate the Nevada Computer Crimes Law."). The jury heard all the evidence in this case and based on the straight forward language of the jury instructions, must have either concluded that defendants believed that they did not have authorization to take the support documents in the manner that they did, which was through the use of automated downloading tools that they specifically agreed not to use when they accessed the database website, or exceeded any perceived authorization by using automated downloading tools in such an aggressive and continuous manner so that their use of the website was higher than *all other Oracle software customers combined* during the period from November 2008 through January 2009.

Finally, defendants' entire argument boils down to the nonsensical assertion that their clients granted them the right to do something the clients themselves did not have the right to do, namely, log on to Oracle America's website and take material from the website with prohibited automated tools. This argument is completely untenable. If an Oracle customer did not have

permission or authority from Oracle America to take documents from the website through the use

of automated downloading tools, then that same client could not subsequently give defendants

permission to engage in the same conduct that they were prohibited from engaging in. Thus,

viewing the evidence presented at trial in the light most favorable to Oracle as the non-moving

party, the court finds that the jury's verdict finding that defendants violated both the CDAFA and

the NCCL when they used, or caused to be used, automated downloading tools on Oracle

America's website in violation of the website's Terms of Use is sufficiently supported by the

evidence. Accordingly, the court shall deny this challenge to the jury's verdict.

F. Damages Award

Defendants' fourth challenge to the jury verdict is that neither the CDAFA or the NCCL

permit for the jury's multi-million dollar damages award. *See* ECF No. 913. In addition to the

$27,000 in investigation and repair damages incurred by Oracle for investigating the website's

shutdown and resetting the database servers, the jury awarded Oracle $14.4 million in additional

damages as a result of defendants' conduct under both the CDAFA and the NCC; split between

Oracle America ($8.8 million) and OIC ($5.6 million). Defendants, outside of their other

challenges in this motion, do not separately challenge the propriety of the $27,000 in investigation

and repair damages award by the jury. ECF No. 913. However, defendants contend that neither

statute authorizes the recovery of the additional $14.4 million in damages awarded by the jury.

Further, defendants argue that even if these damages were recoverable under either statute, the

jury's award of $14.4 million is completely unsupported by the evidence at trial.

1. Available Damages

Under the CDAFA, a plaintiff who suffers "damage or loss" by reason of a violation of the

CDAFA is entitled to "[c]ompensatory damages and injunctive relief or other equitable relief."

CAL. PENAL CODE § 502(e)(1). "Compensatory damages shall include any expenditure reasonably

and necessarily incurred by the owner or lessee to verify that a computer system, computer

network, computer program, or data was or was not altered, damaged, or deleted by the access." *Id*.

Similarly, the NCCL allows for recovery of "damages for any response costs, loss or injury suffered as a result of the crime." NRS § 205.511 "Response costs" are defined as "reasonable costs" that relate to investigating, determining the amount of damage, remedying or preventing future damage, and testing or restoring a computer system.

In their motion, defendants argue that the plain language of these statutes limits the jury award of compensatory damages to only those specified in the statute, namely the $27,000 in reasonable investigation and repair damages awarded by the jury. Defendants contend that the structure of these statutes support a limitation on recoverable damages, because both the CDAFA and the NCCL only specifically mention response and repair costs when defining damages. Further, defendants argue that federal courts, interpreting similar language in the federal computer crimes law statute, have held that a company's lost profits and other corporate economic damages are too far removed from the harm that the statute was designed to protect against to be recoverable under that statute. *See e.g., Farmers Ins. Exchange v. Steele Ins. Agency, Inc.*, 2013 U.S. Dist LEXIS 104606, at *59 (E.D. Cal. July 25, 2013) (holding that damages under the federal computer crimes law are limited to those solely caused by the impairment). Thus, defendants contend that the state statutes only allow the recovery of those damages that are directly associated with the impairment or destruction of computer systems and do not contemplate recovery for subsequent economic damages to a company like those awarded to Oracle in this action. The court disagrees.

The plain, unambiguous language of the CDAFA provides a victim a full range of traditional remedies including "compensatory damages and injunctive relief or other equitable relief." CAL. PENAL CODE § 502(e)(1). Defendants' entire argument is based on a separate sentence which states that "[c]ompensatory damages *shall include* any expenditures reasonably and necessarily incurred by the owner or lessee to verify" system integrity after a violation. *Id*. (emphasis added). Defendants want to limit a plaintiff's "compensatory damages" to only the verification and repair damages specifically mentioned by the CDAFA. In doing so they misconstrue the phrase "shall include" as a limitation to damages under the CDAFA. Defendants'

14

interpretation of the statute is directly contrary to the statute's plain language which allows for the recovery of "compensatory damages and injunctive or other equitable relief." *See* CAL. PENAL CODE § 502(e)(1). Further, under the rules of statutory construction, the word "includes" is a word of enlargement, not limitation. *Patton v. Sherwood*, 152 Call. App. 4th 339, 346 (2007). Thus, the court finds that the plain terms of the CDAFA allows for the recovery of all compensatory damages, including economic damages. The court's interpretation of the CDAFA is supported by other courts that have examined the statute. *See AtPac, Inc. v. Aptitude Solutions*, 730 F. Supp. 2d 1174, 1184 (E.D. Cal. 2010) (holding that loss under the CDAFA includes both the reasonable costs incurred by the victim as well as lost revenue or other damages incurred as a result of the defendants' conduct.

Similarly, the court finds that the NCCL similarly permits recovery of a company's economic damages. Under the NCCL, a civil plaintiff has a private right of action to recover "[d]amages for any response costs, loss or injury suffered as a result of the crime." NRS § 205.511(1). Damages for "loss" or "injury" under the statute clearly include economic damages that are a result of a defendant's violating conduct.

2. **Evidence at Trial**

Defendants next argue that even if economic damages are recoverable under the CDAFA and the NCCL, the jury's $14.4 million damages award cannot be sustained because there was no evidence to support Oracle's claim that it lost customers or company profits *because* of their use of automated downloading tools during a three month period from November 2008 through January 2009. Defendants contend that at trial Oracle offered nothing but a conclusory and demonstrably illogical theory for lost profits, and failed to identify a single customer it lost solely as a result of defendants' automated downloading. Thus, defendants argue that there is no evidence supporting an award of $14 .4 million in lost profits, especially in light of the fact that the jury found that Oracle was not entitled to any lost profits damages on its claim for copyright infringement.

///

15

The court has reviewed the documents and pleadings on file in this matter and finds that the jury had sufficient evidence from which to infer that defendants' unauthorized taking of technical and support files caused Oracle to suffer economic damages including losing clients to defendants' services. At trial, Oracle proffered evidence from its damages expert Elizabeth Dean ("Dean") that Oracle America suffered $27,000 in investigation and repair damages due to defendants' conduct. Dean also calculated Oracle America's and OIC's lost profits from the loss of customers who were serviced by defendants because of defendants' unauthorized taking and use of data from Oracle America's website at $14.4 million split between $8.8 million for Oracle America and $5.6 million for OIC. Dean attributed this loss of clients to customers who left Oracle for defendants because defendants were able to provide the necessary library of technical and support files to service that customer's software at a fraction of the price charged by Oracle.

Other evidence presented at trial supported and corroborated Dean's expert testimony. For example, the evidence presented at trial established that Rimini's clients needed a library of support materials in order to properly utilize the software licensed from Oracle. If was further established at trial that it was critical that Rimini be able to offer its new customers the entirety of Oracle's library of support materials, particularly in the 2008-09 period when Rimini was still trying to establish itself as a serious third-party support competitor. At that time, Rimini was under intense pressure to complete the downloading of all support materials - even those not needed or requested by the clients whose login Rimini used to access Oracle America's website - before its newest customers' software support service contracts with Oracle ended. Further, defendants advertised to prospective clients Rimini's ability to completely service all Oracle Enterprise software programs by explaining that Rimini had the full library of support and technical materials for all software programs on its own systems and without a need to access Oracle America's website. Because of defendants' conduct in taking entire libraries of support materials, prior Oracle clients were able to have their Oracle software serviced by defendants at a 50% discount from Oracle's services. Further, Dean testified that the ability for defendants to offer clients full software

16

support services by having complete access to Oracle's technical and support services on their own

systems without having to access Oracle America's website before servicing that client caused

tangible economic loss and injury to Oracle. Taking all of the evidence in the light most favorable

to Oracle as the non-moving party, the court finds that there was sufficient evidence for the jury to

conclude that Oracle suffered $14.4 million in economic damages as a result of defendants'

conduct. *See Pavao*, 307 F.3d at 918.

G. Constitutionality Challenges

Defendants' last challenge to the jury verdict relates to the constitutionality of both the

CDAFA and the NCCL. In particular, defendants contend that the statutes are unconstitutional on

their face, and are also unconstitutional as applied in this action. The court shall address both

challenges to the constitutionality of the statutes below.

1. Facial Challenge

"The void-for-vagueness doctrine requires that a penal statute define the criminal offense

with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a

manner that does not encourage arbitrary and discriminatory enforcement." *Kolender v. Lawson*,

461 U.S. 352, 357 (1983). If a statute does not meet both of these requirements, then it "fails to

meet the requirements of the Due Process Clause," and is unconstitutional on its face. *City of

Chicago v. Morales*, 527 U.S. 41, 56 (1999).

In their Rule 50(b) motion, defendants argue that both the CDAFA and NCCL are

unconstitutionally vague because they do not define the underlying offense with sufficient

definiteness for a person to understand that their conduct is a crime. *See* ECF No. 913. Defendants'

argument is without merit. Contrary to defendants' challenge, courts that have interpreted the

CDAFA have determined that the statute is not unconstitutionally vague. *See e.g., People v.

Hawkins*, 98 Cal. App. 4th 1428, 1443 (2002) (holding that Section 502 is "sufficiently clear to

avoid constitutional problems"); *Craigslist, Inc. v. 3taps, Inc.*, 964 F. Supp. 2d 1178, 1184 (N.D.

Cal. 2013) (holding that there are "no serious constitutional doubts" about the CDAFA);

17

Christensen, 801 F.3d 970, 994 (applying the CDAFA in a criminal case without constitutional hesitation). Further, although no court has specifically dealt with the constitutionality of the NCCL, many courts have relied on this statute for civil and criminal cases without constitutional hesitation. *See e.g., Microsoft Corporation v. Al Mutairi*, Case No. 2:14-cv-0987-GMN-GWF (2015 U.S. Dist. LEXIS 95541) (Dist. Nev. 2015). Therefore, the court finds that these statutes are not facially unconstitutional.

2. As-applied Challenge

Defendants also contend that the CDAFA and NCCL are unconstitutional as applied in this action, and thus, the court should overturn the jury's verdict on these claims.

An as-applied challenge to the constitutionality of a statute is a challenge "under which the [party] argues that a statute, even though generally constitutional, operates unconstitutionally as to him or her because of the [party's] particular circumstance." *Tex. Workers' Comp. Comm'n v. Garcia*, 893 S.W.2d 504, 518 (Tex. 1995). The relevant inquiry in an as-applied challenge is whether the challenged statute is unconstitutionally vague "as applied to the particular facts at issue" such that the challenging party did not have sufficient notice that his or her conduct would be a violation of the statute. *Holder v. Humanitarian Law Project*, 561 U.S. 1, 18 (2010). Thus, the question for the court to determine in an as-applied challenge is whether defendant had notice that his or her particular conduct could be a violation of the statute. *See United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (identifying notice as the key issue for a court in determining whether to extend liability to private computer and company policies).

In their motion, defendants argue that it would be unconstitutional to hold them civilly liable under these statutes for simply violating the Terms of Use of a website that is written by, enforced by, and solely under the control of, Oracle. Defendants contend that because Oracle has the sole authority to change the terms of the Terms of Use at any time and without any notice to a party using the Oracle America website, then violating the Terms of Use cannot constitutionally support a violation of either the CDAFA or the NCCL.

Defendants' argument effectively asks the court whether they can be found liable under a criminal statute that allows for civil penalties for taking information from a website without authorization when the power to grant, restrict, change, or revoke that authorization is solely within the control of the plaintiff seeking damages under the statute. The short answer is yes. *See Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178, 1184 (N.D. Cal. 2013). The long answer, and the inquiry for the court in this action, involves an examination of the notice Oracle communicated to defendants that using automated downloading tools on the website was not authorized.

The Ninth Circuit's interpretation of the phrase "without authorization" in the federal Computer Fraud and Abuse Act "confirms that computer owners have the power to revoke the authorization that they grant." *Craigslist, Inc.*, 964 F. Supp. 2d at 1183 (citing *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009)). This issue is how well that revocation of authorization is communicated to the defendants. *Id*. at 1184. In *Nosal*, the Ninth Circuit was concerned with companies using private use policies, like Oracle America's Terms of Use, to criminalize behavior and hold defendants liable under criminal abuse statutes because "most people are only dimly aware of and virtually no one reads or understands" such private use policies and the control of what is authorized under the policies is solely within the control of the party seeking damages for a violation of the statutes. *See Nosal*, 676 F.3d at 860-861. The constitutional concerns are alleviated, however, when a defendant has sufficient notice that an owner of a computer system like Oracle America has changed the permission or authorizations granted on its website. *Craigslist, Inc.*, 964 F. Supp. 2d at 1184. "The notice issue becomes limited to how clearly the website owner communicates the [change in website permissions]." *Id*.

Here, defendants have no basis to suggest that they lacked notice that their downloading of technical and support materials from Oracle America's website through the use of automated downloading tools was "without authorization." First, it is undisputed that defendants knew Oracle America changed its website's Terms of Use to prohibit automated downloading tools in February 2007, more than a year and half before defendants engaged in the prohibited conduct. Second, even

if defendants were unsure that their conduct was unauthorized when they began using the prohibited automated downloading tools in November 2008, defendants were sufficiently put on notice that their conduct was unauthorized when Oracle sent several cease-and-desist letters to defendants and banned Rimini's original IP address from accessing the website. Defendants have never suggested that those measures did not put them on notice that their conduct was improper; indeed, defendants had to circumvent Oracle's blocking measures to continue accessing the website and downloading the support files. In such a situation, the "average person" will not unwittingly violate the law because an ordinary average person does not innocently "bypass an IP block set up to enforce a banning" from a website for violation of the website's Terms of Use. *Craiglist, Inc.*, 964 F. Supp. 2d at 1184. Rather, a person of ordinary intelligence would understand Oracle's actions to be a revocation of authorization to access the website and continue using automated downloading tools to take files from the website, and thus have fair notice that further access of the website and the continued use of such automated tools was "without authorization." *Id*. at 1186. Therefore, the court finds that neither the CDAFA nor the NCCL are unconstitutional as applied to defendants' conduct in this action. Accordingly, the court shall deny defendants' Rule 50(b) motion.

IT IS THEREFORE ORDERED that defendants' renewed motion for judgment as a matter of law (ECF No. 913) is DENIED.

IT IS SO ORDERED.

DATED this 13th day of June, 2016.

_____
LARRY R. HICKS
UNITED STATES DISTRICT JUDGE