

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

DOMAIN NAME COMMISSION
LIMITED,

Plaintiff,

v.

DOMAINTOOLS, LLC,

Defendant.

NO. C18-0874RSL

ORDER GRANTING IN PART
DEFENDANT’S MOTION TO
DISMISS

This matter comes before the Court on defendant’s “Motion to Dismiss Pursuant to FRCP 12(b)(1) and 12(b)(6).” Dkt. # 64. Plaintiff is a New Zealand non-profit corporation that regulates the use of the .nz top level domain, including registering new domain names and responding to inquiries regarding registrants. Defendant collects domain and registrant information from around the world, stores the information, and uses its current and historic databases to sell monitoring and investigative services and products to the public. Plaintiff alleges that the way defendant accessed .nz domain and registrant information before June 6, 2018, any and all access after that date, and its continuing storage and use of the domain and registrant information violates the Computer Fraud and Abuse Act (“CFAA”) and the Washington Consumer Protection Act (“CPA”). Defendant seeks dismissal of the statutory

ORDER GRANTING IN PART
DEFENDANT’S MOTION TO DISMISS - 1

1 claims.¹

2 The question for the Court on a motion to dismiss is whether the facts alleged in the
3 complaint sufficiently state a “plausible” ground for relief. *Bell Atl. Corp. v. Twombly*, 550 U.S.
4 544, 570 (2007). All well-pleaded allegations are presumed to be true, with all reasonable
5 inferences drawn in favor of the non-moving party. *In re Fitness Holdings Int’l, Inc.*, 714 F.3d
6 1141, 1144-45 (9th Cir. 2013). If the First Amended Complaint (Dkt. # 54) fails to state a
7 cognizable legal theory or fails to provide sufficient facts to support a claim, however, dismissal
8 is appropriate. *Shroyer v. New Cingular Wireless Servs., Inc.*, 622 F.3d 1035, 1041 (9th Cir.
9 2010).

10
11 Having reviewed the memoranda submitted by the parties and heard the arguments of
12 counsel, the Court finds as follows:

13
14 **A. Computer Fraud and Abuse Act, 18 U.S.C. § 1030**

15 As relevant to this litigation, the CFAA prohibits “intentionally access[ing] a computer
16 without authorization or exceed[ing] authorized access,” 18 U.S.C. § 1030(a)(2), as well as
17 “intentionally access[ing] a protected computer without authorization” and causing “damage and
18 loss,” 18 U.S.C. § 1030(a)(5)(C). Plaintiffs argue that defendant is liable under both provisions
19 because it accessed the .nz servers in ways and for purposes that violated plaintiff’s terms of use
20 and continued to access the .nz servers after its right of access had been expressly revoked.

21
22 Plaintiff’s terms of use prohibited use of Port 43, a communication channel through
23 which users can query plaintiff’s servers regarding specific .nz domain names, to send high
24

25 ¹ Plaintiff has also asserted a breach of contract claim, regarding which the Court entered a
26 preliminary injunction on September 12, 2018. Dkt. # 43. The preliminary injunctive relief was affirmed
27 on appeal, and defendant is not seeking dismissal of the contract claim.

1 volume queries to the .nz servers with the effect of downloading or collecting all or part of the
2 .nz register, to access the .nz register in bulk, to store or compile .nz domain data to build up a
3 secondary register, and/or to publish historical or non-current versions of the .nz data. Dkt. # 54-
4 1 at 18. On November 2, 2017, plaintiff sent defendant a cease-and-desist letter notifying
5 defendant that it had violated plaintiff’s terms of use and demanding that it “immediately cease
6 and desist accessing .nz WHOIS servers or using and publishing .nz WHOIS data except as
7 permitted by the [terms of use].” Dkt. # 54-1 at 24. When defendant continued to access the .nz
8 servers in ways that plaintiff felt violated the limited license it had granted defendant, plaintiff
9 sent a June 6, 2018, letter revoking defendant’s right to access the .nz servers entirely. Dkt. # 54-
10 1 at 30. Plaintiff alleges that defendant accessed the .nz servers after the June 6, 2018,
11 revocation. Dkt. # 54 at ¶ 106.²
12

13
14 Plaintiff argues that defendant’s access to the .nz server in ways that violated plaintiff’s
15 terms of use prior to June 6, 2018, constitutes both access “without authorization” and in excess
16 of authorized access. Dkt. # 54 at ¶¶ 74-79 and 104. Plaintiff also argues that defendant’s queries
17 to the .nz servers after plaintiff revoked defendant’s right of access was “without authorization.”
18 Dkt. # 54 at ¶ 106. Plaintiff alleges that defendant’s unlawful conduct caused plaintiff “loss in an
19 amount far in excess of the \$5,000 statutory minimum during each relevant one-year period.”
20 Dkt. # 54 at ¶ 107.
21
22

23
24 ² Defendant challenges the adequacy of this allegation, but it is more than enough to give rise to
25 a plausible inference that defendant continued to access the .nz servers after June 6, 2018. *Twombly* does
26 not require that plaintiff include in its complaint a log indicating the times and dates on which such
27 access occurred, nor has defendant demanded such specificity as to the pre-June 6 access allegations. If,
28 as appears to be the case, defendant is contesting the veracity of the post- June 6 access allegation, it
may not do so in the context of this motion to dismiss.

1 **1. “Without Authorization”**

2 The CFAA does not contain a definition of “without authorization.” The Ninth Circuit
3 has, therefore, applied the ordinary, common meaning of “authorization,” concluding that one is
4 authorized to access a computer when the owner of the computer gives permission to use it.
5 *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132-33 (9th Cir. 2009). *See also hiQ Labs, Inc.*
6 *v. LinkedIn Corp.*, 938 F.3d 985, 999 (9th Cir. 2019) (“We have held in another context that the
7 phrase “without authorization” is a non-technical term that, given its plain and ordinary
8 meaning, means accessing a protected computer without permission.”) (internal quotation marks
9 and citation omitted). A defendant runs afoul of the “without authorization” provisions of the
10 CFAA “when he or she has no permission to access a computer or when such permission has
11 been revoked explicitly. Once permission has been revoked, technological gamesmanship or
12 enlisting of a third party to aid in access will not excuse liability.” *Facebook, Inc. v. Power*
13 *Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016). The Ninth Circuit has rejected the argument
14 that permission or authorization to access a computer is automatically withdrawn when the user
15 violates a duty owed to the owner of the computer. Rather, whether access is authorized or
16 unauthorized “depends on actions taken by the employer.” *Brekka*, 581 F.3d at 1134-35. If the
17 computer owner has not affirmatively rescinded the defendant’s right to access the computer,
18 any existing authorization/permission remains. *Id.*

19 Prior to June 6, 2018, defendant had permission to access the .nz servers, albeit with
20 limitations imposed on the manner in which and purposes for which that access could be
21

1 exercised.³ That permission was revoked on June 6, 2018. Taking plaintiff’s allegations of
2 access as true, the Court finds that defendant accessed the .nz servers with authorization prior to
3 June 6, 2018, and without authorization after that date.⁴

4 2. “Exceeds Authorized Access”

5
6 The CFAA defines “exceeds authorized access” to mean “to access a computer with
7 authorization and to use such access to obtain or alter information in the computer that the
8 accessor is not entitled to so obtain or alter.” 18 U.S.C. § 1030(e)(6). In *United States v. Nosal*,
9 676 F.3d 854 (9th Cir. 2012), the Ninth Circuit acknowledged that this language could be read in
10 two ways. The first would encompass situations in which a person’s authorization to access a
11 computer is limited to certain files, programs, or databases, but he or she “hacks” into other areas
12 of the computer without permission. In the alternative, the language could refer to a person who
13
14

15
16 ³ At one point in the First Amended Complaint, plaintiff alleges that, prior to June 6, 2018, it
17 deployed blocking technology “to limit and prevent [defendant’s] access to the .nz WHOIS service and
18 the WHOIS service.” Dkt. # 54 at ¶ 104. The suggestion that plaintiff attempted to deprive defendant of
19 any and all access to its servers prior to June 6, 2018, is contradicted by other allegations of the
20 complaint (*see* Dkt. # 54 at ¶¶ 3, 40, 67, and 105) and does not, therefore, give rise to a plausible
21 inference that defendant’s authorization or permission to access the .nz servers and the data contained
22 therein was revoked prior to June 6, 2018. If, in fact, plaintiff took steps prior to June 6, 2018, to entirely
23 exclude defendant from accessing the .nz server through passwords, ISP blocking, or other technological
24 means and defendant hacked its way into the servers, plaintiff may file a motion for leave to amend its
25 complaint using the procedures set forth in LCR 15.

26 ⁴ The Court declines to rule upon defendant’s brief argument (which it expounded upon during
27 oral argument) that plaintiff cannot revoke its authorization to access the .nz servers “given the public
28 nature of the information at issue.” Dkt. # 64 at 17. *hiQ Labs*, the case cited by defendant, suggests that
the reference to “without authorization” limits the scope of statutory protection to information
delineated as private through the use of a permission or authentication requirement, such as a password.
938 F.3d at 1001. Plaintiff’s allegations, taken as a whole, give rise to a plausible inference that access
through Port 43 is different from and limited in ways that access through plaintiff’s public website is
not. The Court declines to scrutinize these inferences further without more of a factual record and
additional assistance from the parties.

1 has unrestricted access to a computer, but who accesses the files, programs, or databases in a
2 way or for a purpose that is proscribed by the owner. *Id.* at 856-57. The Ninth Circuit was
3 concerned that the second interpretation would “transform the CFAA from an anti-hacking
4 statute into an expansive misappropriation statute,” making “everyone who uses a computer in
5 violation of computer use restrictions - which may well include everyone who uses a computer”
6 liable under the CFAA. *Id.* at 857.⁵ The Ninth Circuit held that, whereas the “without
7 authorization” clause of § 1030(c)(2) applies to outside hackers with no rights or authority to
8 access the computer at all, the “exceeds authorized access” clause applies to inside hackers
9 “whose initial access to a computer is authorized but who access unauthorized information or
10 files.” *Id.* at 858. It sided with “the growing number of courts” who recognize that the CFAA
11 “target[s] the unauthorized procurement or alteration of information, not its misuse or
12 misappropriation.” *Id.* at 863 (quoting *Shamrock Foods Co. v. Gast*, 535 F. Supp.2d 962, 965 (D.
13 Ariz. 2008)).

14
15
16 Plaintiff argues that once it specifically and individually reminded defendant on
17 November 2, 2017, that its access to the .nz servers was subject to plaintiff’s terms of use,
18 further access in violation of the terms of use exceeded defendant’s authorization under the
19 analysis set forth in *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016), and
20

21
22 ⁵ The Ninth Circuit recognized that “[w]hen we access a web page, commence a download,
23 post a message on somebody’s Facebook wall . . . or do the thousands of other things we routinely do
24 online, we are using one computer to send commands to other computers at remote locations. Our access
25 to those remote computers is governed by a series of private agreements and policies that most people
26 are only dimly aware of and virtually no one reads or understands.” *Id.* at 861. Because “website owners
27 retain the right to change the terms [of use] at any time and without notice,” an interpretation of
28 “exceeds authorized access” that encompassed violations of use restrictions would mean that “behavior
that wasn’t criminal yesterday can become criminal today without an act of Congress, and without any
notice whatsoever.” *Id.* at 862.

1 *Ticketmaster LLC v. Prestige Entm't W., Inc.*, 315 F. Supp.3d 1147, 1171 (C.D. Cal. 2018).
2 *Facebook* does not support plaintiff's claim of a CFAA violation prior to June 6, 2018. In that
3 case, Facebook issued a cease-and-desist letter notifying defendant that it was no longer
4 authorized to access Facebook's computers. *Facebook*, 844 F.3d at 1067 n.3. In light of the
5 "explicit revo[cation of the] authorization for *any* access," the Ninth Circuit found that
6 defendant's access following receipt of the notice was without authorization and a violation of
7 the CFAA. *Id.* at 1068 (emphasis in original). Plaintiff's November 2, 2017, letter did not revoke
8 defendant's access to the .nz servers, it simply reminded defendant that access was subject to the
9 terms of use.
10

11
12 *Ticketmaster*, on the other hand, supports plaintiff's argument, but the Court declines to
13 adopt its analysis. In *Ticketmaster*, the ticket seller made tickets available to the public on its
14 website subject to terms of use that barred the use of robots, programs, and other automated
15 devices ("bots") to make purchases. Defendants used bots to purchase large quantities of tickets
16 for resale. The district court recognized that simply violating Ticketmaster's terms of use did
17 not, standing alone, constitute a violation of the CFAA under *Nosal*. The district court
18 distinguished *Nosal*, however, on the ground that Ticketmaster had sent defendants an
19 individualized cease-and-desist letter informing them that their access was restricted to that
20 which conforms to Ticketmaster's terms of use. In the court's view, this letter "was, in effect, an
21 individualized access policy that revoked authorization upon breach of the policy. . . . [It was]
22 the violation of the terms of the Letter, not of Ticketmaster's Terms of Use, on which the Court
23 base[d] its finding of a well-pled CFAA claim." 315 F. Supp.3d at 1170-71.
24
25

26 The Court respectfully disagrees. Permission or authorization to access a computer does
27

1 not evaporate simply because the user has violated a duty owed to the owner of the computer.
2 *See Brekka*, 581 F.3d at 1134-35 (rejecting the Seventh Circuit’s reasoning in *Int’l Airport Ctrs.,*
3 *LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), and requiring the employer to rescind the
4 defendant’s right to use the computer before potential criminal liability under the CFAA will
5 attach). “The CFAA was enacted to prevent intentional intrusion into someone else’s computer -
6 specifically, computer hacking.” *hiQ Labs*, 938 F.3d at 1000. The forbidden conduct is
7 analogous to “breaking and entering,” where defendant has unlawfully intruded into otherwise
8 inaccessible computers (or portions thereof) in a form of trespass. *Id.*(quoting H.R. Rep. No. 98-
9 894, at 20 (1984)). The Ninth Circuit has already determined that the rule of lenity demands that
10 the “exceeds authorized access” prong of the CFAA be given a narrow interpretation so as to
11 criminalize unauthorized access to a computer (or part thereof), not the misuse of authorized
12 access. *Nosal*, 676 F.3d at 863. *See also hiQ Labs*, 938 F.3d at 1000 (recognizing that the Ninth
13 Circuit has “rejected the contract-based interpretation of the CFAA’s prohibitions). This Court is
14 not at liberty to second guess the Ninth Circuit’s resolution of the issue, nor is it persuaded that
15 simply repeating or referencing the existing use restrictions in a letter changes the scope of
16 authorized access in a material way.
17
18
19

20 For all of the foregoing reasons, the Court finds that the allegations of the First Amended
21 Complaint do not support a plausible inference that defendant exceeded its authorization to
22 access the .nz servers (as that phrase has been interpreted by the Ninth Circuit) prior to June 6,
23 2018.

24 **3. “Damage or Loss”**

25 The CFAA provides a private right of action to “[a]ny person who suffers damage or loss
26
27

1 by reason of a violation of this section,” 18 U.S.C. § 1030(g), as long as the violation causes
2 “loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value,” 18
3 U.S.C. § 1030(c)(4)(A)(i)(I). “Damage” is defined as “any impairment to the integrity or
4 availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8). “Loss” means
5 “any reasonable cost to any victim, including the cost of responding to an offense, conducting a
6 damage assessment, and restoring the data, program, system, or information to its condition prior
7 to the offense, and any revenue lost, costs incurred, or other consequential damages incurred
8 because of interruption of service.” 18 U.S.C. § 1030(e)(11). Thus, while “damage” covers harm
9 to the integrity or availability of the data or information on the computer, “loss” refers to the
10 monetary injuries imposed on plaintiff by defendant’s conduct.
11
12

13 Plaintiff alleges that it “has suffered loss in an amount far in excess of the \$5,000
14 statutory minimum during each relevant one-year period, in an amount to be proved at trial. This
15 loss includes, without limitation, the costs [plaintiff] has incurred in investigating and
16 responding to [defendant’s] misconduct.” Dkt. # 54 at 25.⁶ For the reasons discussed above, the
17 only potential violations of the CFAA occurred after June 6, 2018, and plaintiff’s allegations
18 provide no basis on which to allocate the alleged losses between the pre- and post-revocation
19 periods. Plaintiff filed its initial complaint on June 15, 2018, less than two weeks after it revoked
20 defendant’s right to access the .nz servers: the identical loss allegation is in that document, again
21
22

23
24 ⁶ Defendant points out that, in order to survive a motion to dismiss the claim under 18 U.S.C.
25 § 1030(a)(5)(C), plaintiff must allege facts giving rise to a plausible inference that its unauthorized
26 access to the .nz servers caused both “damage and loss” in the conjunctive. *See NovelPoster v. Javitch*
27 *Canfield Group*, 140 F. Supp.3d 954, 961 (N.D. Cal. 2014). Because plaintiff has not adequately alleged
28 the jurisdictional amount, the Court need not determine whether “damage” has been alleged for
purposes of § 1030(a)(5)(C).

1 with no indication of any events or actions giving rise to post-revocation “loss.” *See* Dkt. # 1 at
2 ¶ 105. The Court finds that the allegations do not give rise to a plausible inference that
3 defendant’s alleged violations of the CFAA - limited as they are to the post-June 6, 2018, period
4 - caused damage or loss in excess of \$5,000.
5

6 **B. Washington Consumer Protection Act (“CPA”), RCW 19.86**

7 To prevail on a CPA claim, plaintiff must prove an “(1) unfair or deceptive act or
8 practice; (2) occurring in trade or commerce; (3) public interest impact; (4) injury to plaintiff in
9 his or her business or property; [and] (5) causation.” *Hangman Ridge Training Stables, Inc. v.*
10 *Safeco Title Ins. Co.*, 105 Wn.2d 778, 780 (1986). Plaintiff alleges that defendant’s efforts to
11 circumvent the rate limiting and use restrictions plaintiff imposed to protect the data on its
12 servers was “unfair or deceptive,” that defendant engaged in these unfair acts in order to create
13 and sell its products and services, that the public’s interest is impacted because consumers are
14 deprived of their privacy, and that plaintiff has incurred expenses and suffered injury to
15 reputation and good will as a result. Dkt. # 54 at ¶¶ 109-112.
16

17 The CPA is a consumer protection statute that applies to both “unfair” and “deceptive”
18 acts and practices. The wrongs about which plaintiff complains - that defendant improperly
19 gathered data from plaintiff’s computers and repackaged it into products and services for its own
20 customers - are not deceptive insofar as they do not have “the capacity to deceive a substantial
21 portion of the public.” *Hangman Ridge*, 105 Wn.2d at 785. Plaintiff has identified no
22 representation or act defendant directed at the public, much less one that has the capacity to
23 deceive a substantial portion of the public. Rather, plaintiff alleges that the information
24 defendant publishes to its customers may be outdated and the customers could obtain more
25
26
27

1 accurate information directly from plaintiff. Dkt. # 54 at ¶ 88. Absent some indication that
2 defendant advertises its wares as “100% accurate” or “the most up-to-date registry information
3 available,” merely offering for sale a product or service that could be bettered is not a deceptive
4 act.⁷

5
6 The CPA also prohibits unfair acts and practices, even if they are not deceptive. *Klem v.*
7 *Wash. Mut. Bank*, 176 Wn.2d 771, 787 (2013). Although the full contours of “unfair acts” under
8 the CPA have not yet been established, the Supreme Court of Washington has cited federal law
9 for the proposition that a “practice is unfair [if it] causes or is likely to cause substantial injury to
10 consumers which is not reasonably avoidable by consumers themselves and not outweighed by
11 countervailing benefits.” *Klem*, 176 Wn.2d at 787 (quoting 15 U.S.C. § 45(n)) (alteration in
12 original). Plaintiff describes the unfair acts at issue here as harvesting and storing .nz registrant
13 information by means of cyber misconduct, particularly the circumvention of protective
14 technologies and the breach of plaintiff’s terms of use. Dkt. # 68 at 25. Circumventing a server’s
15 protective technologies can be an unfair method of competition, act, or practice.⁸ Defendant
16
17

18
19 ⁷ At oral argument, plaintiff argued that defendant disguised itself to avoid the technological
20 defenses plaintiff erected and to hide its improper bulk queries and downloads. While disguising oneself
21 may well be deceptive, plaintiff has not raised a plausible inference that anyone but itself was deceived
22 by the disguise.

23 ⁸ Courts around the country have found that companies that hold sensitive personal and financial
24 information but fail to take adequate steps to secure their servers may be liable under various consumer
25 protection statutes. *See FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 247 (3rd Cir. 2015); *Gordon*
26 *v. Chipotle Mexican Grill, Inc.*, 344 F. Supp.3d 1231 (D. Colo. 2018); *Buckley v. Santander Consumer*
27 *USA, Inc.*, 2018 WL 1532671, at *4 (W.D. Wash. Mar. 29, 2018) (CPA); *Veridian Credit Union v.*
28 *Eddie Bauer, LLC*, 2017 WL 5194975, at *13 (W.D. Wash. Nov. 9, 2017) (CPA); *In re Anthem, Inc.*
Data Breach Litig., 162 F. Supp.3d 953 (N.D. Cal. 2016); *In re Michaels Stores Pin Pad Litig.*, 830 F.
Supp.2d 518 (N.D. Ill. 2011). If the failure to adequately protect sensitive customer data can be deemed
unfair, it is hard to imagine that circumventing the security systems imposed by the holder of the data in
its (unsuccessful) effort to prevent the misuse of the information would be considered “fair.”

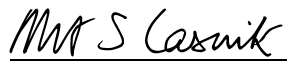
1 argues, however, that the allegations of the complaint do not give rise to a plausible inference
2 that defendant’s conduct “is likely to cause substantial injury to consumers.” *Klem*, 176 Wn.2d
3 at 787 (quoting 15 U.S.C. § 45(n)). The information defendant obtained was, defendant points
4 out, available to the public through plaintiff’s website and Port 43 at the time it was obtained,
5 and there is no indication that .nz registrants had any reason to believe that plaintiff would keep
6 the information they provided confidential.⁹ Nevertheless, .nz registrants did have reason to
7 believe that their information would not be harvested and stored, such that they could cancel
8 their registration or alter their privacy selections and limit what information would be publicly
9 available going forward: what plaintiff calls a consumer’s “dynamic privacy interest.” Consumers
10 who chose to participate in plaintiff’s enhanced individual registrant privacy option when it was
11 offered were therefore harmed by defendant’s prior downloading/storing of information that,
12 while previously available to the public, was now unavailable. At that point, defendant had
13 access to - and sold - information it had unfairly downloaded and stored, depriving consumers of
14 their ability to control the privacy of certain information in accordance with their agreements
15 with plaintiff.

16
17
18
19 The Court finds that plaintiff has raised a plausible inference that defendant’s use of bulk
20 queries to download and store registrant information in violation of protective technologies and
21 terms of use is an unfair act in trade or commerce that is likely to cause substantial injury to
22 consumers which is not reasonably avoidable by consumers themselves and not outweighed by
23 countervailing benefits.

24
25
26 ⁹ For most of the relevant period, registering for a .nz domain name involved an
27 acknowledgment that all registrant information would be available to the public.

1 For all of the foregoing reasons, defendant's motion to dismiss the CFAA and CPA
2 claims is GRANTED in part. Because this matter continues as to plaintiff's breach of contract
3 and CPA claims, leave to amend will not be blindly granted. If plaintiff believes it can,
4 consistent with its Rule 11 obligations, amend the complaint to remedy the pleading and legal
5 deficiencies in its CFAA claim, it may file a motion to amend and attach a proposed pleading for
6 the Court's consideration.
7

8
9 Dated this 26th day of March, 2020.

10 
11 _____
12 Robert S. Lasnik
13 United States District Judge
14
15
16
17
18
19
20
21
22
23
24
25
26
27