PAUL B. SALVATY (171507)
PSalvaty@winston.com
WINSTON & STRAWN LLP
333 S. Grand Ave.
Los Angeles, CA 90071-1543
Telephone: (213) 615-1700
Facsimile: (213) 615-1750

ABBE DAVID LOWELL (pro hac vice)
AbbeLowellPublicOutreach@winston.com
WINSTON & STRAWN LLP
1901 L St., N.W.
Washington, DC 20036-3508
Telephone: (202) 282-5000
Facsimile: (202) 282-5100

BRYAN M. SULLIVAN (209743)
bsullivan@earlysullivan.com
ZACHARY C. HANSEN (325128)
EARLY SULLIVAN WRIGHT GIZER & McRAE LLP
6420 Wilshire Boulevard, 17th Fl.
Los Angeles, CA 90048
Telephone: (323) 301-4660
Facsimile: (323) 301-4676

Attorneys for Plaintiff
ROBERT HUNTER BIDEN

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

ROBERT HUNTER BIDEN,

Plaintiff,

vs.

GARRETT ZIEGLER, an individual, ICU, LLC, a Wyoming limited liability company d/b/a Marco Polo, and DOES 1 through 10, inclusive,

Defendants.

Case No. 2:23-cv-07593-HVD-KS

Honorable Hernan D. Vera
Magistrate Judge Karen L. Stevenson

PLAINTIFF'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS PURSUANT TO RULES 12(b)(1), 12(b)(2), 12(b)(3), AND 12(b)(6) OF THE FEDERAL RULES OF CIVIL PROCEDURE AND SECTION 425.16 OF THE CALIFORNIA CODE OF CIVIL PROCEDURE

Hearing Date: March 21, 2024
Time: 10:00 a.m.
Place: 5B

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. INTRODUCTION

Defendants Garrett Ziegler ("Ziegler") and ICU, LLC ("ICU") readily admit that for months, if not years, they have been accessing, tampering with, and manipulating Plaintiff Robert Hunter Biden's data without his authorization or consent. Yet they insist they cannot be held responsible for their actions because, according to them, they accessed, tampered with, and manipulated a "copy" of Plaintiff's data while it was stored on a "hard drive" they obtained from a third party, rather than accessing Plaintiff's data while it was stored on a "computer" or "device" that was "owned" and "exclusively controlled" by Plaintiff himself.

Defendants' Motion to Dismiss Pursuant to Fed. R. Civ. P. 12(b)(1), 12(b)(2), 12(b)(3) and 12(b)(6) and Section 425.16 of the California Code of Civil Procedure ("Motion") is baseless. For one thing, Defendants' ownership-and-control argument is contrary to Ninth Circuit and California law. Neither the federal Computer Fraud and Abuse Act ("CFAA") nor California's Comprehensive Computer Data Access and Fraud Act ("CCDAFA") requires Plaintiff to plead or prove "ownership" or "control" of the physical "computer" or "device" that Defendants accessed. With respect to the CFAA, the Ninth Circuit specifically has held that ownership or control of a "computer" is not required and that a plaintiff may seek redress where, as here, he is "proximately harmed by unauthorized access, particularly if [he has] rights to the *data* stored on it." *See Theofel v. Farey-Jones,* 359 F.3d 1066, 1078 (9th Cir. 2004) (emphasis added). Similarly, the CCDAFA prohibits knowingly accessing and without permission taking and using "any data" from a computer; it does not require a plaintiff to own or control a physical device. Cal. Pen. Code § 502(c)(2); *see also* Cal. Pen. Code § 502(e)(1) (authorizing civil action by "owner or lessee of . . . *data* who suffers damage or loss by reason of a violation") (emphasis added).

At this early stage, Plaintiff needs only to allege "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal,* 556 U.S. 662, 678 (2009) (*quoting Bell Atl. Corp. v. Twombly,* 550 U.S. 544, 570 (2007); *see also Park v. Thompson,* 851 F.3d 910, 918 (9th Cir. 2017) (generally, court must accept factual allegations as true and view them in light most favorable to plaintiff)). Here, Plaintiff has pled uncontroverted facts to support the Court's exercise of federal question and diversity jurisdiction, which precludes dismissal under Rule 12(b)(1).

Plaintiff also has alleged—and readily can establish—extensive facts to support the Court's exercise of personal jurisdiction over Defendants, which prevents dismissal under Rule 12(b)(2). With respect to Defendants' arguments under Rule 12(b)(6), Plaintiff has factually alleged each of his claims in precisely the manner specified by the Ninth Circuit. Defendants spend most of the Motion arguing the merits, which is improper at this stage, particularly because Defendants' counternarrative is contrary to the Complaint's well-pleaded allegations, unsupported by evidence, and inconsistent with facts that have come to light in other proceedings. *See, e.g., King v. Rubenstein*, 825 F.3d 206, 214 (4th Cir. 2016) (internal citation and quotation omitted) (Rule 12(b)(6) motion generally cannot be used to "resolve contests surrounding the facts, the merits of a claim, or the applicability of defenses").

To the extent the Motion is supported by admissible evidence, that evidence bolsters Plaintiff's position, not Defendants'. Defendants present a sworn declaration from Ziegler in which he admits under oath—perhaps without realizing the consequences of doing so—that Defendants spent months "locating" Plaintiff's passwords and then used one or more of those passwords to access Plaintiff's password-protected data. Ziegler states:

> Also contained on the external hard drive given to me were files containing passcodes, which are essentially similar in function to passwords designed to allow access to password-protected files. Although it took months of examination, we were able to locate the passcode which allowed access to the iPhone backup file. Those files existed on the external hard drive when it was first given to me.

See Declaration of Garrett Ziegler ("Ziegler Decl.") ¶ 21. This surprisingly frank admission proves Defendants' unlawful data access as a matter of law. It is precisely the type of "hacking" activity that the statutes are intended to punish. *See, e.g., Facebook, Inc. v. Power Ventures, Inc.*, 2010 WL 3291750, at *11 (N.D. Cal. July 20, 2010) (access that circumvents technical or code-based barriers is "without permission" as a matter of law); *Mintz v. Mark Bartelstein & Assocs.*, 906 F. Supp. 2d 1017, 1032 (2012) (use of plaintiff's password without consent to access email constituted CCDAFA violation as a matter of law).

Finally, Defendants' arguments based on California's anti-SLAPP statute fail because Plaintiff's claims do not "arise from" protected First Amendment activity. Plaintiff sued Defendants for their

unlawful and unauthorized access to data, not for their use of the data to engage in data-related speech. This is clear from the first paragraph of the Complaint. (Compl. ¶ 1 ("While Defendant Ziegler is entitled to his extremist and counterfactual opinions, he has no right to engage in illegal activities to advance his right-wing agenda")). Moreover, Plaintiff's claims are not subject to anti-SLAPP dismissal because they are likely to succeed at trial. Accordingly, the Court should deny Defendants' Motion.

II. BACKGROUND

A. The Parties

Plaintiff is an attorney and businessman and is the second-born son of President Joseph R. Biden, Jr. Although Plaintiff is and always has been a private citizen, political opponents of President Biden have used him as a surrogate to attack his father. For the past several years, Plaintiff has been the target of relentless personal attacks and the subject of countless baseless conspiracy theories, particularly from extreme right-wing members of Congress and the media.

Defendant Ziegler is a former Trump White House aide who worked, from February 2019 until January 2021, as a Policy Analyst and, later, as an Associate Director of the Office of Trade and Manufacturing Policy under the supervision of Dr. Peter Navarro. Since having his White House credentials revoked in or around January 2021, Ziegler, by his own admission, has devoted most of his waking time and energy to accessing, tampering with, manipulating, altering, copying, and otherwise using data contained on a copy of a hard drive that Defendants claim to be of Plaintiff's "laptop" computer. (Compl. ¶¶ 15-16.)

On or about July 8, 2021, Defendant Ziegler organized Defendant ICU and caused Defendant ICU to begin doing business under the name "Marco Polo." (*Id.* ¶ 20.) Defendants claim to have spent at least 13 months—from September 2021 through October 2022—"analyzing the voluminous material from the Biden Laptop," and their unlawful access, manipulation, and analysis of Plaintiff's data continues to this day. (*Id.* ¶ 21.)

B. Plaintiff's Allegations of Defendants' Illegal Data Access

The precise manner by which Defendants obtained Plaintiff's data remains unclear. (Compl. ¶¶ 17-18.) In their Motion, Defendants are vague on this point, stating only that Ziegler "received a copy from an associate of former New York City mayor Rudy Giuliani." (Ziegler Decl. ¶ 5.) In published

reports, Ziegler has claimed to have obtained one copy of a hard drive containing Plaintiff's data from Jack Maxey, a former co-host on convicted felon Steve Bannon's *War Room* podcast, and another copy of a hard drive containing Plaintiff's data from another source. (Compl. ¶ 18.) Defendants will have to explain how many copies of Plaintiff's data they received and from whom, as well as the precise data they came to possess, during discovery in this case.

Regardless of how Defendants, without his permission, came to possess Plaintiff's data, once Plaintiff's data was in their custody, they accessed, tampered with, analyzed, and manipulated the data over an extended period of time. Defendant Ziegler used Plaintiff's data to create a voluminous report entitled "Report on the Biden Laptop" ("Report"), which Defendants first published on or about October 19, 2022. (Compl. ¶ 22.) Defendants have sold and sent copies of the Report throughout the United States, including California. In addition, in or around May 2022, Defendants used Plaintiff's data to create what Defendant Ziegler has described as "an online searchable database of 128,000 emails found on the Biden Laptop." (*Id.*) Plaintiff has never authorized or consented to any access of his data by any Defendant or anyone working with any Defendant at any time or for any purpose. To the contrary, Plaintiff notified Defendants that they are not authorized to access any of his data, that they should cease doing so, and that they should return any of Plaintiff's data to Plaintiff immediately. (Compl. ¶ 30.)

Defendants regularly brag about their illegal access of Plaintiff's data in interviews with members of the media, on social media, and on right-wing podcasts. For example, in December 2022, Ziegler described the activities of his team, which he said includes "digital forensics folks," as follows: "[I]t took us a year to go through [the data] . . . Usually, when you have this much data to go through, it's as if it's after a presidential library has been opened, right?" (Compl. ¶¶ 23-24.) In another interview published in or around June 2023, Ziegler discussed his and his team's efforts to create a website to house "almost 10,000 photos" that he claims to have extracted from Plaintiff's data. (*Id.*)

According to Ziegler, Defendants spent "a couple of months" going through photos stored in Plaintiff's data, organizing and modifying the photos (through what he characterizes as "redactions"), and subjecting the data to a "photo viewing app" to allow Defendants and others to "view the metadata in the photos." (*Id.* ¶ 25.) Ziegler claims these activities are designed to allow members of the public who log onto Defendants' website and access Defendants' servers "to be able to see where the photo

was taken, what time it was taken, if it has latitude and longitude coordinates attached to it. . . They're going to be able to see if it has metadata like aperture, lighting." (*Id.*) Ziegler further has stated that Defendants' efforts to upload videos from Plaintiff's data to Defendants' website required more time and effort than uploading photos from Plaintiff's data because Defendants needed "to use AI tools" on the data to "censor" portions of videos that Defendants consider to be "pornographic." (*Id.* ¶ 26.)

The data Defendants have unlawfully accessed, manipulated, and damaged includes tens of thousands of emails, thousands of photos, and dozens of videos and recordings. (*Id.* ¶ 27.) The data also includes Plaintiff's credit card details, Plaintiff's financial and bank records, and information of the type contained in the files of a consumer reporting agency. (*Id.*) At least some of the data originally was stored on Plaintiff's iPhone and backed-up to Plaintiff's iCloud storage. (*Id.* ¶ 28.) Defendants gained unlawful access to Plaintiff's iPhone data by circumventing technical or code-based barriers that were specifically designed and intended to prevent such access. (*Id.*)

In an interview that occurred in or around December 2022, Defendant Ziegler bragged that Defendants had hacked their way into data purportedly stored on or originating from Plaintiff's iPhone: "And we actually got into [Plaintiff's] iPhone backup, we were the first group to do it in June of 2022, we cracked the encrypted code that was stored on his laptop." (*Id.* ¶ 29.) After "cracking the encrypted code that was stored on [Plaintiff's] laptop," Defendants illegally accessed the data and then uploaded it to their website, where it remains accessible to this day. (*Id.*) It appears that data Defendants uploaded to their website from Plaintiff's encrypted "iPhone backup," like data Defendants uploaded from their copy of the hard drive of the purported "laptop," has been manipulated, tampered with, altered, and/or damaged by Defendants. (*Id.*)[1]

Defendants have refused to comply with Plaintiff's demands to cease and desist. As recently as September 2023, Defendant Ziegler declared on social media that efforts by Plaintiff to serve him with legal process in the future would be met with violence: "If the US pResident's son sends a proxy [i.e., a process server] to illegally trespass on my property I will blow their f---ing brains out." (*Id.* ¶ 31.)

[1] The nature and extent of Defendants' manipulation, tampering, alteration, and damage to Plaintiff's data, either from their copy of the hard drive of the claimed "Biden laptop" or from Plaintiff's encrypted "iPhone backup" (or from some other source), is unknown to Plaintiff due to Defendants' continuing refusal to return the data to Plaintiff. (Compl. ¶ 29.)

C. Plaintiff's Complaint, and Defendants' Motion to Dismiss

Plaintiff commenced this lawsuit on September 13, 2023. The Complaint alleges one federal claim and two state claims: (1) Violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; (2) Violation of the California's Comprehensive Computer Data Access and Fraud Act ("CCDAFA"), Cal. Penal Code § 502; and (3) Violation of California's Unfair Competition Law ("UCL"), Business & Professions Code §§ 17200 *et seq.*

In their Motion, Defendants seek dismissal of the Complaint pursuant to Rules 12(b)(1), 12(b)(2), 12(b)(3), and 12(b)(6) of the Federal Rules of Civil Procedure and pursuant to California's Anti-SLAPP statute, Cal. Civ. Proc. Code § 425.16. The Motion should be denied in its entirety.

III. ARGUMENT

A. The Court Has Subject Matter Jurisdiction Because Plaintiff Has Alleged Violation of a Federal Statute and Because There Is Complete Diversity Under 28 U.S.C. § 1332(a).

Defendants' first argument is that the Complaint must be dismissed for lack of subject matter jurisdiction because Plaintiff "cannot show that any federal statutory violation has occurred" and because Plaintiff "lacks standing" to assert any of his claims. *See* Mot. at 4-6. Defendants' position appears to be based on a fundamental misunderstanding of federal jurisdiction and a failure to read or acknowledge the jurisdictional allegations of the Complaint.

Plaintiff pleads two separate bases for subject matter jurisdiction: (1) federal question jurisdiction based on Defendants' violation of the CFAA; and (2) complete diversity of citizenship. (Compl. ¶¶ 6-8); *see also* 18 U.S.C. § 1030(g); 28 U.S.C. § 1332(a). Defendants inexplicably ignore diversity jurisdiction in their Motion. They do not dispute the sufficiency of Plaintiff's diversity allegations; and they make no attempt to show that, as a factual matter, the requirements for diversity jurisdiction are not present in this case. To the extent their papers address diversity-related issues at all, the Motion bolsters Plaintiff's allegations of diversity and supports the exercise of jurisdiction under 28 U.S.C. § 1332(a). (*See, e.g.,* Ziegler Decl. ¶¶ 4, 17 (confirming Defendants' Illinois and Wyoming residences).)

Even if diversity jurisdiction did not exist, the Court would have subject matter jurisdiction based on Plaintiff's claim for violation of the CFAA. The CFAA is a federal statute that "subjects to criminal liability anyone who 'intentionally accesses a computer without authorization or exceeds authorized access,' and thereby obtains computer information." *Van Buren v. United States,* 141 S. Ct. 1648, 210 L. Ed. 2d 26, 33 (2021), *citing* 18 U.S.C. § 1030(a)(2). "It defines the term 'exceeds authorized access' to mean '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.'" *Id.*, *citing* 18 U.S.C. § 1030(e)(6). Subsection (a)(2)'s prohibition initially barred accessing only certain financial information. *Id*. But it "has since been expanded to cover any information from any computer 'used in or affecting interstate or foreign commerce or communication.'" *Id., citing* 18 U.S.C. § 1030(e)(2)(B). "As a result, the prohibition now applies—at a minimum—to all information from all computers that connect to the internet." *Id.*, *citing* 18 U.S.C. §§ 1030(a)(2)(C), (e)(2)(B). In addition to criminal penalties, violators face civil liability under the CFAA's private cause of action, which allows persons suffering "damage" or "loss" to sue for money damages and equitable relief. *Id., citing* 18 U.S.C. § 1030(g).

Defendants claim federal question jurisdiction should be deemed not to exist in this case because Plaintiff "cannot show that any federal statutory violation has occurred." *See* Mot. at 4. At this stage, Plaintiff is not required to prove the merits of his federal claim. Plaintiff need only show his federal claim is not "absolutely devoid of any merit." *See, e.g., Custom Packaging Supply, Inc. v. Phillips*, 2015 WL 8334793 (C.D. Cal. Dec. 7, 2015) (*citing In re Nucorp Energy Sec. Litig.*, 772 F.2d 1486, 1490 (9th Cir. 1985); *see also Hagans v. Lavine,* 415 U.S. 528, 538, 548 (1974) (federal claim is insubstantial only if it is clearly foreclosed by prior decisions or otherwise patently without merit). Merely alleging that a federal claim lacks merit is not sufficient to affect jurisdiction. *Shapiro v. McManus*, 577 U.S. 39, 45 (2015); *see also Benalcazar v. Genoa Twp*., 1 F.4th 421, 425 (6th Cir. 2021) (explaining that the "threshold question" is "do the federal questions raised by this complaint legitimately create federal court jurisdiction because they are not so frivolous as to be a contrived effort to create such jurisdiction?"); *McCoy v. Iberdrola Renewables, Inc.*, 760 F.3d 674, 681 (7th Cir. 2014) ("When it comes to invoking federal jurisdiction, the bar is low.").

Here, Defendants argue that Plaintiff's CFAA claim is "frivolous," that Plaintiff "lacks standing," and that Plaintiff somehow is "not a real party in interest" because "[n]either the CFAA nor the CCDAFA authorize a party whose data has been copied to assert a civil action over any computer, device or system not in their possession." Mot. at 5. This argument, which appears throughout the Motion, is simply wrong. Neither the CFAA nor the CCDAFA contain any requirement that Plaintiff must "own," "possess," or "control" the physical device that Defendants accessed. To the contrary, both statutes authorize Plaintiff to assert claims under the circumstances of this case. *See* 18 U.S.C. § 1030(g) (extending civil remedy to "any person" who suffers damage or loss); Cal. Pen. Code § 502(e)(1) (extending civil remedy to owners of "data" who suffer damage or loss). Likewise, neither statute insulates Defendants from liability merely because they claim to have accessed a "copy" of Plaintiff's data on a "hard drive" obtained from a third party, rather than accessing data stored on a physical device "exclusively" owned and controlled by Plaintiff. *See, e.g.,* 18 U.S.C. § 1030(a)(2) and (a)(4); Cal. Pen. Code § 502. Defendants' ownership-and-control argument is inconsistent with both the language and purpose of the CFAA and the CCDAFA, and it has been rejected by the Ninth Circuit. *See Theofel,* 359 F.3d at 1078 (holding "district court erred by reading ownership or control requirement into the [CFAA]").

Finally, Defendants attack subject matter jurisdiction on the grounds that Plaintiff's CFAA claim is untimely. This argument fails for multiple reasons. For one thing, statutes of limitations "ordinarily are not jurisdictional." *Sebelius v. Auburn Reg'l Med. Ctr.,* 568 U.S. 145, 154 (2013). Where, as here, the statute of limitations is not expressly identified as "jurisdictional," it must be treated as not affecting the court's subject matter jurisdiction. *Id.* at 153-154*; see also Musacchio v. United States*, 577 U.S. 237, 246 (2016) (time bar jurisdictional "only if Congress has 'clearly stated' that it is"). Moreover, the untimeliness of a federal claim would not deprive the Court of subject matter jurisdiction over state law claims, where, as here, Plaintiff's state claims are timely, and the requirements of diversity jurisdiction have been met.

More fundamentally, Defendants' untimeliness argument fails because Plaintiff asserted his claim for violation of the CFAA "within 2 years of the date of the act complained of or the date of the discovery of the damage," as required. 18 U.S.C. § 1030(g). Plaintiff alleges—and Defendants

concede—that Defendants spent many months "accessing" and "analyzing" the data, from at least "September 2021 through October 2022." (Compl. ¶ 21; *see* Ziegler Decl. ¶ 6.) Defendants have refused to cease and desist, and they appear to be continuing to engage in unlawful data access. Thus, by their own admission, most, if not all, of Defendants' "acts" of unauthorized access to Plaintiff's data occurred within the statute; and separate CFAA violations are continuing to accrue every day. Defendants' limitations defense provides no basis for dismissal, whether under Rule 12(b)(1) or otherwise. *See Phreesia, Inc. v. Certify Glob., Inc.*, 2022 WL 911207, at *10 (D. Md. Mar. 29, 2022) (holding "separate accrual" approach applies to CFAA claims and refusing to dismiss where Plaintiff "alleges potential CFAA violation occurring within the limitations period").

B. The Court Has Personal Jurisdiction Over Defendants, and Venue in the Central District of California Is Proper.

1. Plaintiff Easily Establishes Specific Personal Jurisdiction Here.

A district court's exercise of personal jurisdiction over a nonresident defendant comports with due process when the defendant has at least minimum contacts with the forum and subjecting the defendant to suit in the forum will "not offend traditional notions of fair play and substantial justice." *See, e.g., Ayla LLC v. Ayla Skin Pty Ltd.*, 11 F.4th 972, 979 (9th Cir. 2021) (internal citation omitted). Specific jurisdiction exists where a defendant (1) purposefully directed his activities toward or purposefully availed himself of conducting business with the forum; (2) the plaintiff's claims "arise out of or result from" the defendant's forum-related activities; and (3) the exercise of jurisdiction is reasonable. *See id.* The plaintiff bears the burden on the first two prongs, and if they are established, the defendant "must come forward with a 'compelling case' that the exercise of jurisdiction would not be reasonable." *Id.* (quoting *Boschetto v. Hansing,* 539 F.3d 1011, 1016 (9th Cir. 2008)). And where a motion to dismiss is based on written materials rather than an evidentiary hearing, "the plaintiff need only make a prima facie showing of jurisdictional facts" to defeat the motion. *Id.* at 978 (quoting *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 800 (9th Cir. 2004).

Where, as here, Plaintiff's claims sound in tort, courts use the "purposeful direction" test to evaluate the first prong, which is satisfied where the defendant (1) committed an intentional act, (2) expressly aimed at the forum state, (3) causing harm that the defendant knows is likely to be suffered in

the forum state. *See Ayla LLC*, 11 F.4th at 980 (citing *Calder v. Jones*, 465 U.S. 783 (1984)). Under this test, courts focus "on the forum in which the defendant's actions were felt, whether or not the actions themselves occurred within the forum." *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 433 F.3d 1199, 1206 (9th Cir. 2006). Although express aiming requires "conduct directly targeting the forum" beyond mere knowledge that the plaintiff lives in the forum state, *Ayla LLC*, 11 F.4th at 980, "*all* of a defendant's contacts with the forum state" must be examined in the jurisdictional analysis. *Yahoo! Inc.* 433 F.3d at 1207 (emphasis added).

Defendants do not dispute that Plaintiff lives in California and suffered the relevant harm in California due to Defendants' wrongful hacking and publication of his private data. Nor could they, given that Defendants' "Report" repeatedly mentions Plaintiff's purported conduct in California and Plaintiff's California residency has been publicized since at least 2019. (Declaration of Gregory A. Ellis ("Ellis Decl.") Ex. A.) And although the moving papers try to cast Defendants' contacts with California as being limited to the availability of their purportedly passive website within the state (Mot. at 8, 10-11), the evidence belies that notion. Rather, Ziegler's own declaration, his own internet postings, and statements out of his own mouth all demonstrate that Defendants repeatedly and expressly aimed their conduct at California in their wrongful exploitation of Plaintiff's private data.

Ziegler's Declaration Admissions Establishing California Contacts: Ziegler notes that the "Report" Defendants prepared using Plaintiff's data is available at the website bidenreport.com. (Ziegler Decl. ¶ 8 & n.1.) Prominently displayed on that website is a "Purchase" button, allowing users to spend $50.00 for a hardcopy of the report. (Ellis Decl. ¶ 6 & Ex. E.). Clicking the purchase button, in turn, links to a purchase page operated by Stripe.com, a California-based entity whose purchase terms are governed by California law. *See* www.stripe.com/legal/consumer, Section 12. The fact that the website allows purchases precludes any claim by Defendants that their website is purely passive, as their own case authority establishes. *See Stomp, Inc. v. NeatO, LLC*, 61 F. Supp. 2d 1074, 1078 (C.D. Cal. 1999) (cited in Motion at. 11, finding website not passive where it allowed users to purchase the product at issue).[2]

[2] Defendants' other "website" cases are similarly distinguishable, or help Plaintiff. In *Pebble Beach Co. v. Caddy*, the defendant hotel's website only included an inquiry form and did not allow visitors to make reservations. *See* 453 F.3d 1151, 1154 (9th Cir. 2006). The website in *Cybersell, Inc. v. Cybersell, Inc.* likewise only allowed users

Ziegler also admits that "over six million unique IP addresses have reviewed the *Report* on the *Marco Polo* website," (Ziegler Decl. ¶ 12) and that "less than ten percent of *Marco Polo's* supporters reside in California." (*Id.* ¶ 16.) Although Ziegler uses the intentionally-vague term "supporters," the figures in his declaration indicate that nearly 600,000 people may have viewed the Report from California. And if Defendants argue that "supporters" refers to financial donors, the Ninth Circuit has found as few as 13 subscribers of a publication in California were sufficient to support personal jurisdiction in the tort context. *See Gordy v. Daily News, L.P.*, 95 F.3d 829, 831, 834 (9th Cir. 1996) (13 to 18 subscribers – or 0.0017% of *New York Daily News* subscriber base – were sufficient to support personal jurisdiction); *see also College Source, Inc. v. AcademyOne, Inc.*, 653 F.3d 1066, 1071 (9th Cir. 2011) (reversing grant of motion to dismiss in case alleging violations of CFAA and CCDAFA, holding personal jurisdiction existed where 300 subscribers in California).[3]

Defendants' Express Direction Toward California in Preparing the Report: In multiple interviews with right-wing broadcasters, Ziegler claimed that he and his team[4] called "each and every person that is

---

to email the defendant. *See* 130 F.3d 414, 415-416 (9th Cir. 1997). In *Schwarzenegger*, the defendant had a website that was "available for viewing" but apparently did not allow for purchases through the site. 374 F.3d at 799. And in *Bancroft & Masters v. Augusta Nat'l, Inc.*, the Ninth Circuit *reversed* a grant of a motion to dismiss, holding that personal jurisdiction existed where the defendant had a website available in California and also sent a cease and desist letter from Georgia to Virginia that was intended to affect plaintiff in California. 223 F.3d 1082, 1087-88 (9th Cir. 2000). Here, Defendants acted in both Illinois and California to affect Plaintiff in California.

[3] Moreover, Ziegler has indicated in interviews that he tracks *where* and *who* accesses the Marco Polo website – and has called out site visitors from California. In his interview on the Steve Bannon *War Room* podcast, Ziegler stated that a California state legislator had visited one of Marco Polo's websites to search for her name. (Ellis Decl. Ex. B at 2.)

Ziegler's assertions about Defendants' website views and support from California also demonstrate that the Court should exercise its discretion to allow jurisdictional discovery, should it still have questions about jurisdiction even after reviewing Plaintiff's evidence. *See, e.g., Orchid Biosciences, Inc. v. St. Louis Univ.*, 198 F.R.D. 670, 672-73 (S.D. Cal. 2001) (noting that courts have broad discretion in allowing jurisdictional discovery, citing multiple authorities). Here, discovery would be appropriate to address the following issues, at a minimum: the total number of Defendants' financial supporters based in California; the percentage of their total financial supporters based in California; the total amount of money donated from California; the percentage of Defendants' monetary donations emanating from California; the total number of unique website viewers from California; the percentage of unique website viewers from California; the number and percentages of website purchases of hardcopies of the Report emanating from California locations; and the number of California residents Ziegler sent hardcopies of the Report to in his "carpet-bombing" campaign, discussed *infra.*

[4] It is unclear whether the "team" of individuals who assisted Defendants with their data-related activities includes any California residents. In his declaration, Ziegler attests he has "hired no employees or independent contracts [sic] to conduct business in California, nor do any of *Marco Polo*'s board members reside in California." (Ziegler Decl. ¶ 13.) But this careful wording leaves open many potential California connections, including the possibility that some aspects of Defendants' unlawful data-related activities occurred in California and/or were perpetrated by California residents who were assisting Defendants in a capacity other than as "employees or independent

named in this report" in the course of its preparation. (Ellis Decl. Exs. C at 13; D at 8-9.) These contacts included numerous California residents. The Report includes tables of purported "crimes," several of which supposedly took place in "C.D. Cal." and "N.D. Cal." Of those, the table sets out, in the "Who" column, fifteen telephone numbers with California area codes. (*Id*. Ex. E at 233-35, 400-01.) Ziegler knew full well these contacts were based in California. Ziegler also has bragged about an elaborate "catfishing" operation he and his associates performed on Plaintiff's attorney and friend, California resident Kevin Morris, in preparing the Report. (Ellis Decl. Exs. F at 4-5; G at 9-12.) The operation included Defendants using "two private investigators" to "look into Kevin Morris for about a month" (presumably in California), posing to Morris as someone friendly to Plaintiff "over the course of weeks," and then "feeding" Morris with what Ziegler now claims to be "false information" about manipulation of the data belonging to Plaintiff. (Ellis Decl. Ex. G at 10.)

These sixteen-plus contacts are more than enough to establish express, purposeful direction toward California. *See, e.g., College Source, Inc.*, 653 F.3d at 1078-79 (9th Cir. 2011) (pointing to defendant's calls to plaintiff in California as supporting jurisdiction); *Calder*, 465 U.S. at 785, 788 (using sources of information in California supported exercise of jurisdiction); *Gordy*, 95 F.3d at 831 (using California sources for defamatory article supported exercise of jurisdiction).

Ziegler's Express Direction Toward California in Promoting the Report: On or about December 16, 2023, Ziegler posted a photo of himself on Instagram in front of the Chateau Marmont Hotel in West Hollywood, holding a copy of the Report. (Ellis Decl. Ex. H.) Likewise, on or about November 1, 2022, Ziegler posted a Rumble video of himself in San Francisco, entitled "Report on the Biden Laptop: CA Field Trip," again promoting the Report. (*Id*. Ex. I.) On top of physically entering into California, Ziegler's social media posts reflecting his entry into California support the exercise of jurisdiction. *See Yue v. Yang*, 62 Cal. App. 5th 539, 543, 547-48 (2021) ("California-focused" social media messages, including statement that defendant "arrived in California," supported jurisdiction). Ziegler also reached into California virtually, appearing on a YouTube broadcast run by two Southern California residents, to promote the Report. (Ellis Decl. Ex. G; *see Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1020

contractors." The location of Defendants' "team" members is another appropriate topic for jurisdictional discovery.

(9th Cir. 2002) (advertising in forum state, combined with even a passive website, justified exercise of jurisdiction). Defendants also sent the Report to a substantial number of Californians. In a podcast with pardoned felon Roger Stone, Ziegler said that he sent the Report to "all 4,000 contacts on Hunter's laptop." (Ellis Decl. Ex. D at 8.) In addition to the sixteen California contacts noted above, Ziegler thus sent the Report to other California residents identified in the Report, including but not limited to an FBI agent in the San Francisco field office. (*Id*. Ex. E at 22.) Defendants even sent the Report to the personal residence of one of Plaintiff's California-based attorneys. (*Id*. ¶ 12.) Likewise, Ziegler told conservative commentator Eric Metaxas that he was "carpet bombing" the Report by sending it to media outlets around the country, likely adding to the total copies Defendants sent to California. (*Id*. Ex. C at_1-2.) Courts in the Ninth Circuit have held that as few as thirteen to eighteen mailings into the forum state are sufficient to support jurisdiction—fewer than what Defendants admit to sending here. *See e.g.*, *Gordy*, 95 F.3d at 834 ("13 or 18 subscriptions are enough to count as a connection when distributed in the state where the target is domiciled and will suffer most from damage to his reputation."). Taken together, all these contacts with California demonstrate "physical entry into the State – either by the defendant in person . . . goods, mail, *or some other means*," *Christie v. Nat'l Inst. for Newman Studies*, 258 F. Supp. 3d 494, 501 (D.N.J. 2017) (emphasis in original, exercising personal jurisdiction in CFAA case), and are more than sufficient to satisfy the "purposeful availment. . . purposeful direction of activities at the forum; or. . . some combination thereof" to create personal jurisdiction. *Yahoo, Inc.!,* 433 F.3d at 1206.

The Claim "Arises Out of" Defendants' California Contacts: To satisfy the "arising out of" prong, a plaintiff need only show that a "direct nexus exists between the defendant's contacts and the cause of action." *See Fireman's Fund Ins. Co. v. Nat'l Bank of Cooperatives*, 103 F.3d 888, 894 (9th Cir. 1996). Ziegler's own statements again evidence that nexus. In his interview with Metaxas, Ziegler expressly tied the credibility of the Report to Defendants' contacts with the persons listed in the Report, claiming that because he called "each and every person that is named in this report" (including the multiple California-based contacts noted above), "It's all real." (Ellis Decl. Ex. C at 13.) Moreover, Plaintiff suffered harm in California from Defendants' misuse of his data, further supporting this prong. *See Rio Props., Inc.*, 284 F.3d at 1021; *see also Yahoo! Inc.*, 433 F.3d at 1206. This harm to Plaintiff is

something that Defendants specifically intended, as is apparent from Ziegler's public statements in which he frequently celebrates his data theft as a "digital colonoscopy." (Ellis Decl. Ex. Jat 2, 7.)

Exercising Jurisdiction in California is Reasonable: Defendants concede that they have the burden of presenting a "compelling case" on the reasonableness prong to avoid the exercise of jurisdiction (Mot. at 10-11), but they do not come close to doing so. They cite the seven-factor "reasonableness" test set forth in *Core-Vent Corp. v. Nobel Indus. AB*, 11 F.3d 1482, 1487-88 (9th Cir. 1993), but only address two of the factors in passing, claiming they "did not intentionally target California" and "the evidence is located in Illinois." Mot. at 12. The first assertion is false, and the second is incomplete. As demonstrated above, Ziegler admits he repeatedly and intentionally targeted California, knowing that Plaintiff lives here. And the fact that Plaintiff lives in California and will offer critical testimony regarding the data at issue and the injuries he suffered due to Defendants' hacking, makes the "evidence" factor a wash at best. Moreover, "California maintains a strong interest in providing an effective means of redress for its residents tortiously injured." *Gordy*, 95 F.3d at 836 (internal citation omitted). Jurisdiction is proper here.

2. Venue Is Proper in the Central District.

Many of the facts supporting personal jurisdiction—Ziegler's calls to people in the Central District, his visit to the Chateau Marmont to promote the Report, and his contacts with webcasters in Southern California—also support venue here. Just as importantly, courts in the Ninth Circuit have determined that in a tort claim, the venue where a plaintiff suffered harm is sufficient to support venue under 28 U.S.C. § 1391(b)(2). *See, e.g., Myers v. Bennett Law Offices*, 238 F.3d 1068, 1076 (9th Cir. 2001); *Sherles v. Fox*, 2018 WL 3046429, at *8 (W.D. Wash. June 20, 2018); *United Tactical Sys. LLC v. Real Action Paintball, Inc.*, 108 F. Supp. 3d 733, 755 (N.D. Cal. 2015). As discussed above, Plaintiff suffered injury in the Central District.

"A plaintiff's choice of venue is generally given substantial weight and a defendant normally 'must make a strong showing of inconvenience to warrant upsetting the plaintiff's choice of forum.'" *Id.* at 751 (quoting *Decker Coal Co. v. Commonwealth Edison Co.*, 805 F.2d 834, 843 (9th Cir. 1986)). Defendants fail to make any showing, let alone a strong one, to defeat venue. Their argument largely parrots general venue factors, but they concede that in evaluating venue, the "entire sequence of events

underlying the claim" is relevant—and that here, the relevant sequence of events includes their website "and publications" of Plaintiff's data. (Mot. at 13.) To the extent they mention *any* facts, Defendants mischaracterize both their own conduct and the nature of Plaintiff's harm. Defendants claim that their only relevant acts were "Ziegler's decisions about what content to post on his website" (*Id.*)—conveniently ignoring the bevy of California contacts Ziegler made in developing and publicizing the content of his website. And in describing the harm at issue, Defendants myopically focus only on the physical location of Plaintiff's devices from which his data was taken, even though Plaintiff suffered other harms, including, for example, investigative costs, and even though the CCDFA allows for the recovery of "compensatory damages" generally. *See* Cal. Penal Code § 502(e)(1); *cf. Myers v. Bennett Law Offices*, 238 F.3d at 1074 (internal citation omitted) (noting that in "'right of privacy' cases the primary damage is the mental distress from having been exposed to public view" and that such harm "can only be felt" where plaintiff resides).[5]

C. Plaintiff's Factual Allegations, As Well As Defendants' Admissions, Support Liability Under Federal and State Anti-Hacking Laws.

Defendants' arguments under Rule 12(b)(6) are similar to their arguments under Rule 12(b)(1). For the most part, they ignore Plaintiff's allegations and insist in sweeping terms that Plaintiff cannot allege any viable theory against them because they accessed a "copy" of Plaintiff's data files rather than accessing a physical "computer" that Plaintiff "owns" or "exclusively controls." *See* Mot. at 15 (arguing no CFAA claim because "Plaintiff alleges no facts which demonstrate Defendants ever accessed any computer, storage, or service which Plaintiff either owns or has exclusive control over"); Mot. at 17 (arguing CCDAFA "requires a defendant to access a computer or device belonging to, or controlled by, the Plaintiff"). This argument is wrong. For the reasons discussed below, Plaintiff properly and sufficiently has alleged each of his claims.

1. Plaintiff Has Pled a Violation of the CFAA.

Plaintiff's first cause of action alleges Defendants violated the CFAA. Defendants seek dismissal of this claim under Rule 12(b)(6) on the grounds that: (1) Plaintiff has not alleged the elements

[5] Ziegler himself tries to protect his own privacy on this Motion: his declaration does not identify his hometown, or where he executed the declaration. (Ziegler Decl.)

of a CFAA violation; (2) Plaintiff has not alleged that Defendants' access was "without authorization"; and (3) Plaintiff does not allege a "recoverable loss" within the meaning of the statute. None of these arguments has merit.

In the Complaint, Plaintiff alleges that Defendants violated the CFAA in three respects: (1) section 1030(a)(2)(A) (unauthorized access of records of "financial institution," "card issuer," or "consumer reporting agency") (Compl. ¶ 34); (2) section 1030(a)(2)(C) (unauthorized access of "information from any protected computer") (Compl. ¶ 35); and (3) section 1030(a)(4) (unauthorized access of protected computer "knowingly and with intent to defraud" where access furthers the fraud and accesser obtains thing of value) (Compl. ¶ 36). Plaintiff seeks redress for these violations pursuant to section 1030(g), which provides in relevant part:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (I), (II), (III), (IV) or (V) of subsection (a)(4)(A)(i).

18 U.S.C. § 1030(g). Here, Plaintiff alleges that Defendants' conduct involves the factor described in subsection (a)(4)(A)(i)(I), which proscribes conduct that causes "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." (Compl. ¶ 37.)

Defendants insist that Plaintiffs have not pled the elements of a CFAA violation, but their arguments are refuted by the CFAA's statutory language and Plaintiff's factual allegations, which align precisely with Ninth Circuit requirements. In *LVRC Holdings,* the Ninth Circuit stated the essential elements of a civil claim for violations of sections 1030(a)(2) and 1030(a)(4);

> "[T]o bring an action successfully under 18 U.S.C. § 1030(g) based on a violation of 18 U.S.C. § 1030(a)(2), [plaintiff] must show that [defendant]: (1) intentionally accessed a computer,[6] (2) without authorization or exceeding authorized access, and that he (3)

[6] The term "computer" is defined broadly to include "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."

> thereby obtained information (4) from any protected computer (if the conduct involved an interstate or foreign communication), and that (5) there was loss to one or more persons during any one-year period aggregating at least $5,000 in value. To bring an action successfully under § 1030(g) based on a violation of § 1030(a)(4), [plaintiff] must show that [defendant]: (1) accessed a 'protected computer,' (2) without authorization or exceeding such authorization that was granted, (3) 'knowingly' and with 'intent to defraud,' and thereby (4) further[ed] the intended fraud and obtain[ed] anything of value,' causing (5) a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

See LVRC Holdings LLC v. Brekka, 581 F3d 1127, 1132 (9th Cir. 2009), *citing* 18 U.S.C. § 1030(a).

Plaintiff has alleged each of these elements in detail. (Compl. ¶¶ 2, 16-18, 20-22, 24-29 (access); ¶¶ 4, 17-18, 21-23, 28-30, 34-36 (without authorization); ¶¶ 22, 24, 27-29 (information obtained); ¶¶ 2, 16, 18-22, 24-26, 28-29, 35-36 (protected computer); ¶ 37 (economic "loss" of type recoverable)). Plaintiff's allegations do not simply recite the elements of a CFAA claim. Rather, they "contain sufficient allegations of underlying facts to give fair notice and to enable [Defendants] to defend [themselves] effectively. . . [and they] plausibly suggest an entitlement to relief, such that it is not unfair to require the opposing party to be subjected to the expense of discovery and continued litigation." *Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011). Nothing more is required. *Id; see also Netapp, Inc. v. Nimble Storage,* 41 F. Supp. 3d 816, 833-834 (N.D. Cal. 2014) (no requirement that CFAA claims be pled with particularity unless "fraudulent conduct is specifically alleged as the basis for the wrongdoing").

Defendants attack the sufficiency of the CFAA claim for Plaintiff's purported failure to plead facts that need not be pled. For example, Defendants insist that Plaintiff cannot state a viable CFAA claim because he has not alleged that "Defendants accessed any computer, storage, or service which Plaintiff either owns or has exclusive control over." *See* Mot. at 15. This is the same erroneous argument Defendants raise under Rule 12(b)(1). As discussed, the CFAA says nothing about

18 U.S.C. § 1030(e)(1). A "protected computer" is a "computer" which is "used in or affecting interstate or foreign commerce or communication…" 18 U.S.C. § 1030(e)(2)(B).

"ownership" and "control" of the physical device that is accessed, and the Ninth Circuit expressly held that ownership and control are not required:

> "The district court erred by reading an ownership or control requirement into the Act. The civil remedy extends to '*[a]ny person* who suffers damage or loss by reason of a violation of this section.' 18 U.S.C. § 1030(g) (emphasis added). '"[T]he word 'any' has an expansive meaning, that is, 'one or some indiscriminately of whatever kind.' . . . Nothing in the provision's language supports the district court's restriction. Individuals other than the computer's owner may be proximately harmed by unauthorized access, particularly if they have rights to data stored on it."

Theofel, 359 F.3d at 1078 (internal citations omitted); *see also* Model Jury Instr. 8.94A.

Defendants also argue it is "questionable whether Plaintiff has adequately alleged that Defendants accessed a 'protected computer'" as defined in the CFAA. *See* Mot. at 14. A "protected computer" is "any computer used in or affecting interstate or foreign commerce or communication." *Id.*; *citing* 18 U.S.C. § 1030(e)(2)(B). The term "computer" includes any "electronic, magnetic, optical, electrochemical, or other high speed data processing device performing . . . storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. . . ." 18 U.S.C. § 1030(e)(1). As the Supreme Court recently explained, the statute's prohibition "now applies—at a minimum—to all information from all computers that connect to the internet." *Van Buren,* 141 S. Ct. at 1652. Here, Plaintiff alleges—and Defendants appear to admit—facts establishing that Defendants accessed a "protected computer." At a minimum, they admit to having accessed a "hard drive" containing data belonging to Plaintiff, including data allegedly stored on Plaintiff's iPhone backup. The data at issue was sent and received over the internet before Defendants accessed it. And after accessing the data, Defendants connected it to the internet so that it could be accessed by the public. They created "an online searchable database of 128,000 emails found on the Biden laptop" as well as a public website to house "almost 10,000 photos"; and they provided the public with metadata and ready access to the password-protected files stored on the iPhone backup. (Compl. ¶¶ 22, 24, 25, 29.) These allegations are more than sufficient to allege Defendants accessed a

"computer" that is "used in or affecting interstate or foreign commerce or communication." *See* 18 U.S.C. §§ 1030(e)(1), (e)(2).

Next, Defendants claim that "Plaintiff does not allege unlawful access to a computer with the meaning of the CFAA." Mot. at 14. But the Complaint includes many factual allegations establishing the unauthorized and unlawful nature of Defendants' data access. Defendants admit to having "accessed" and "analyzed" Plaintiff's data from at least September 2021 until at least October 2022. (Compl. ¶ 21; *see also* Ziegler Decl. ¶ 6.) Plaintiff sent a cease-and-desist demand, which Defendants ignored. (Compl. ¶ 30.) Moreover, Defendants admit that, with respect to at least some data, they gained access by circumventing technical and code-based barriers. (Ziegler Decl. ¶ 21.) Thus, Defendants' own evidence proves their access was "unauthorized" and "without permission" as a matter of law. *See, e.g., Facebook, Inc. v. Power Ventures, Inc.*, *supra,* 2010 WL 3291750, at *11.

Finally, Defendants argue that Plaintiff has failed to allege a "recoverable loss." The CFAA permits the recovery of losses incurred as a result of investigating and responding to Defendants' violations of the CFAA. *See* 18 U.S.C. § 1030(e)(11) ("the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service"). This is precisely what Plaintiff has alleged. Plaintiff alleges that he suffered "direct costs, incurred during any one-year period, of investigating and responding to Defendants violations of the CFAA in excess of $5,000 in value." (Compl. ¶ 37). Contrary to Defendants' claims, Plaintiff is not seeking "legal expenses, lost profits or other consequential damages" in connection with his CFAA claim; Plaintiff's request for those damages is asserted in connection with the state law claims. (*Cf.* Compl. ¶ 37 with Compl. ¶¶ 44-47.)[7]

[7] Defendants raise their statute of limitations defense as a basis for dismissing Plaintiff's CFAA claim under Rule 12(b)(6) as well as under Rule 12(b)(1). For reasons discussed above, the defense is inapplicable because the Complaint alleges—and Defendants appear to admit—that they engaged in numerous acts of unlawful access within the limitations period. *See supra* at 9-10, *citing Phreesia, Inc.*, 2022 WL 911207, at *29; *see also Supermail Cargo, Inc. v. U.S.*, 68 F.3d 1204, 1207 (9th Cir. 1995) ("[A] complaint cannot be dismissed unless it appears beyond doubt that the plaintiff can prove no set of facts that would establish the timeliness of the claim.")

2. Plaintiff Has Pled a Violation of the CCDAFA.

Plaintiff's second cause of action alleges Defendants violated the CCDAFA, which is codified in California Penal Code § 502. The CCDAFA is broader than the CFAA in several respects, and Plaintiff's allegations are more than adequate to state a viable CCDAFA claim.

The Complaint alleges violations of Sections 502(c)(1), (c)(2), (c)(3), and (c)(7) of the CCDAFA, which provide as follows:

> (c) Except as provided in subdivision (h),[8] any person who commits any of the following acts is guilty of a public offense:
>
> (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
>
> (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
>
> (3) Knowingly and without permission uses or causes to be used computer services. . . .
>
> (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

Cal. Pen. Code § 502(c). The statute's private right of action is provided in Section 502(e). *See* Cal. Pen. Code § 502(e)(1).

The Ninth Circuit has distinguished the CCDAFA from the CFAA:

> "The statutes are different. In contrast to the CFAA, the California statute does not require *unauthorized* access. It merely requires *knowing* access. *Compare* 18 U.S.C. § 1030(a)(2) *with* Cal. Penal Code § 502(c)(2). What makes that access unlawful is that the person 'without permission takes, copies or makes use of data on the computer. A plain reading

[8] Subdivision (h) exempts "acts which are committed by a person within the scope of his or her lawful employment." Cal. Pen. Code § 502(h)(1).

of the statute demonstrates that its focus on unauthorized taking or use of information. In contrast, the CFAA criminalizes unauthorized *access*, not subsequent unauthorized use. *United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2015). The term "access" as used by the CCDAFA has been defined broadly, and it plainly includes activities such as those alleged here. *Id.* (term "access" as used in CCDAFA "includes logging into a database with a valid password and subsequently taking, copy, or using the information in the database improperly"); *see also Facebook Inc. v. Power Ventures*, 844 F.3d 1058, 1069 (9th Cir. 2016) (once defendant was told to cease and desist it "knew that it no longer had permission to access [plaintiff's] computers at all").

Defendants argue (again) that Plaintiff cannot state a CCDAFA claim because the statute "requires a defendant to access a computer or device belonging to, or controlled by, Plaintiff." Mot. at 17. For support, they point to the California jury instructions governing CCDAFA claims, claiming that the instruction "specifically requires a showing of ownership and control of the accessed computer as a prerequisite of liability." *Id., citing* CACI No. 1812. The jury instruction says no such thing. The instruction tracks the language of the statute, which applies to anyone who "knowingly accesses" another person's "*data*," not merely to those who access another person's device or computer. *See* CACI No. 1812 (first element requires plaintiff to prove that he is the **[owner/lessee] of the** [*specify computer, computer system, computer network, computer program, and/or data*]; *see also* Cal. Penal Code § 502(e)(1) (authorizing "owner or lessee of computer, computer system, computer network, computer program, or data who suffers damage or loss" to bring civil action).

Defendants also argue that Plaintiff "does not present any facts that Defendants acted without permission." Mot. at 23. But this argument also is based on their mischaracterization of the CCDAFA jury instruction. There is nothing in the instruction that requires Plaintiff to plead or prove "ownership of the hard drive in Defendants' possession [as] a necessary prerequisite to" showing that Defendants' data was "without permission." Liability can arise from proof that Plaintiff owns "data" that Defendants "knowingly accessed" and used "without permission." *See* CACI No. 1812. Moreover, any argument that Defendants acted "with permission" would be specious, given their use of Plaintiff's passwords to access his password-protected files and their disregard of Plaintiff's prelitigation demand to cease and desist.

Finally, Defendants claim "Plaintiff does not allege that he suffered damages" under Section 502. But the Complaint contains factual allegations that contradict their argument. (*See, e.g.*, Compl. ¶¶ 19-21, 25, 27-29, 39-44.) The CCDAFA provides, in addition to any other civil remedy available, the owner of 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." *See* Cal. Pen. Code § 502(e)(1). Compensatory damages include but are not limited to "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*. The statute authorizes an award of reasonable attorneys' fees as well as punitive damages in appropriate cases.

3. Plaintiff Has Pled a Valid UCL Claim.

Defendants present a cursory attack on Plaintiff's third cause of action for violation of California's UCL, arguing primarily that the UCL claim fails because Plaintiff's CFAA and CCDAFA claims are deficient. For reasons already discussed, Plaintiff's CFAA and CCDAFA claims are, in fact, supported by Plaintiff's well-pleaded allegations and Defendants' admissions. Plaintiff is entitled to pursue his UCL claim based on Defendants' unlawful activities. *See Committee on Children's Television, Inc. v. Gen. Foods Corp.,* 35 Cal. 3d 197, 209-10 (1983) (an unlawful business activity includes anything that can properly be called a business practice and that at the same time is forbidden by law); *Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999) (UCL "borrows violations of other laws and treats them as unlawful practices that the unfair competition law makes independently actionable"); *see also Famous Birthdays, LLC v. SocialEdge, Inc.*, 2022 WL 1591723, at *6 (C.D. Cal. Apr. 15, 2022) (denying dismissal of UCL claim because it is "based on all the prior causes of action including . . .the CFAA and CDAFA claims, and those prior claims can be construed to form separate and independent bases for the UCL claim.")

//

//

//

//

D. Plaintiff's Claims Are Not Subject to California's Anti-SLAPP Statute Because the Allegations Do Not Arise from Protected Activity.

Defendants' final argument is that the entire lawsuit should be dismissed pursuant to California's anti-SLAPP statute. Defendants fail to appreciate that the anti-SLAPP statute does not apply to federal claims. *See Hilton v. Hallmark Cards,* 599 F.3d 894, 901 (9th Cir. 2010). To the extent Defendants seek dismissal of Plaintiff's CFAA claim on anti-SLAPP grounds, their motion must be denied. As far as Plaintiff's state law claims, they cannot be dismissed because Defendants cannot make the requisite prima facie showing that anti-SLAPP statute applies and, regardless, the claims have much more than "minimal merit." *See, e.g., Governor Gray Davis Comm. v. Am. Taxpayers Alliance,* 102 Cal. App. 4th 449, 456 (2002) (internal citation omitted) ("Only a cause of action that satisfies *both* prongs of the anti-SLAPP statute—i.e., that arises from protected speech or petitioning activity *and* lacks even minimal merit—is a SLAPP, subject to being stricken under the statute.")

1. Plaintiff's Claims Do Not Arise from Protected Activity.

Defendants cannot make their initial "prima facie" showing that Plaintiff's claims arise from protected activity.

In determining whether Defendants have shown that Plaintiff's claims "arise from" protected activity, "the critical consideration is whether the cause of action is *based* on defendant's protected free speech or petitioning activity." *Navellier v. Sletten,* 29 Cal. 4th 82, 89 (2002). At this first step, courts should "consider the elements of the challenged claim and what actions by the defendant supply those elements and consequently form the basis for liability." *Park v. Bd. of Trustees of California State Univ.*, 2 Cal. 5th 1057, 1063 (2017). "The defendant's burden is to identify what acts each challenged claim rests on and to show how those acts are protected under a statutorily defined category of protected activity." *Bonni v. St. Joseph Health Sys.,* 11 Cal. 5th 995, 1009 (2021) (internal citation omitted). Importantly, "[a]llegations of protected activity that merely provide context, without supporting a claim for recovery, cannot be stricken under the anti-SLAPP statute." *Id.* at 1012*; see also Park,* 2 Cal. 5th at 1060 ("claim may be struck only if the speech or petitioning activity *itself* is the wrong complained of, and not just evidence of liability or a step leading to some different act for which liability is asserted").

Here, Defendants do not even attempt to show that Plaintiff's claims, as alleged in the Complaint, "arise from" Defendants' free speech. Defendants insist that their website is a "public forum," that Plaintiff is a "person in the public eye," and that the so-called "Biden Laptop" has been "a topic of widespread" public interest for some time. Mot. at 21-22. They claim that there have been "thousands of news articles" about the "laptop," and they proudly trumpet the "[m]ore than six million unique IP addresses [that allegedly] have reviewed the report on Defendants' website." *Id.* at 22. But none of these purported "facts" supports application of the anti-SLAPP statute in this case. Plaintiff did not sue Defendants for creating a website, for publishing their "Report," or for any of the many false, defamatory, and malicious statements they have made about Plaintiff over the past two-plus years. Plaintiff carefully pleaded his claims to ensure that they are based solely on Defendants' "accessing, tampering with, manipulating, altering, copying and damaging" of Plaintiff's computer data," and not on Defendants' free speech. Therefore, the anti-SLAPP statute does not apply. *See Malin v. Singer,* 217 Cal. App. 4th 1283, 1303 (2013) (claims based on allegations of illegal wiretapping and computer hacking "do not fit one of the categories of protected activities defined by the Legislature in section 425.16, subdivision (e)" and, therefore, are not subject to anti-SLAPP dismissal); *Gerbosi v. Gaims, Weil, West & Epstein, LLP,* 193 Cal. App. 4th 435, 444 (2011) (alleged criminal conduct including wiretapping and privacy invasions "does not fall within 'protected activity' as defined by the anti-SLAPP statute"); *cf. Hudson Martin v. Forsyth,* 2017 WL 1315576, at *3 (N.D. Cal. Apr. 7, 2017) (defendant's alleged conduct in "*accessing* the firm's computers and *taking* data" did not constitute protected activity; alleged conduct in using the data to gain an advantage in litigation did).

2. Plaintiff's Claims Are Likely to Succeed

Even if Defendants could somehow show that some aspect of Plaintiff's claims arises from protected activity, they would not be entitled to dismissal because the evidence obtained already shows Plaintiff is likely to succeed on the merits of his CCDAFA and UCL claims.

If the court determines that relief is sought based on allegations arising from protected activity, then "the burden shifts to the plaintiff to demonstrate that each challenged claim based on protected activity is legally sufficient and factually substantiated." *Baral v. Schnitt*, 1 Cal. 5th 376, 396 (2016). "The court, without resolving evidentiary conflicts, must determine whether the plaintiff's showing, if

accepted by the trier of fact, would be sufficient to sustain a favorable judgment." *Id.* Where there is a conflict in evidence, the Court may grant the motion only "if, as a matter of law, the defendant's evidence supporting the motion defeats the plaintiff's attempt to establish evidentiary support for the claim." *Hilton,* 599 F. 3d at 901 (internal citations and quotation omitted).

Here, there is ample evidence already to sustain a favorable judgment on Plaintiff's CCDAFA and UCL claims. The evidence available to date indicates that, through means that are not entirely clear, Defendants came to possess data belonging to Plaintiff. (Ziegler Decl. ¶ 5.) After gaining possession of Plaintiff's data, Defendants proceeded to access the data without Plaintiff's authorization or consent. (Declaration of Robert Hunter Biden ("Biden Decl.")[9] ¶¶ 2-3; Ziegler Decl. ¶¶ 5-6, 21.) Defendants' activities included locating Plaintiff's password and using the password to gain access to Plaintiff's password-protected data. (Ziegler Decl. ¶¶ 20-21.) Plaintiff never authorized or consented to Defendants' activities. (Biden Decl. ¶¶ 2-3.) To the contrary, Plaintiff demanded that Defendants cease and desist their unlawful activities, but this demand has been ignored. (Biden Decl. ¶ 3.) Defendants have refused to cease or desist and continuously have accessed, tampered with, and manipulated data belonging to Plaintiff, as proven by Defendant Ziegler's own sworn testimony in this case. (Biden Decl. ¶ 4; Ziegler Decl. ¶¶ 8, 11, 12, and 24.)

IV. CONCLUSION

Much of Defendants' Motion to Dismiss is argument on their version of facts and bald assertions regarding the merits of the claims made. This is not a proper argument for dismissing a well-pled Complaint at this initial stage of a case. Where there is an attack of a legal issue, such as jurisdiction, Defendants misread or misapply the law. This too defeats the argument. For all the reasons addressed in this filing, Defendants' Motion to Dismiss must be denied.

[9] Plaintiff's declaration, filed concurrently herewith, is submitted solely for the purpose of addressing the second prong of the anti-SLAPP inquiry. *See, e.g., Monster Energy Co. v. Schechter*, 7 Cal. 5th 781, 788 (2019) (if defendant meets initial burden, then court moves to second step "accept[ing] the plaintiff's evidence as true, and evaluat[ing] the defendant's showing only to determine if it defeats the plaintiff's claim as a matter of law.").

Dated: February 29, 2024

Respectfully submitted,

WINSTON & STRAWN LLP

By: */s/ Paul B. Salvaty*
Paul Salvaty
Abbe David Lowell
Attorneys for Plaintiff

EARLY SULLIVAN WRIGHT GIZER & McRAE LLP

By: */s/ Bryan M. Sullivan*
Bryan M. Sullivan
Zachary C. Hansen
Attorneys for Plaintiff