UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

Robert Hunter Biden,

Plaintiff,

v.

Garret Ziegler et al.,

Defendants.

Case No. 2:23-cv-07593-HDV (KSx)

ORDER DENYING DEFENDANTS' MOTION TO DISMISS [DKT. NO. 23]

I. INTRODUCTION

This action arises out of alleged violations of federal and state computer fraud statutes. Plaintiff Robert Hunter Biden alleges that Defendants Garrett Ziegler and ICU, LLC illegally accessed, manipulated, and damaged his data without his authorization or consent.

Before the Court is a motion to dismiss the Complaint pursuant to Federal Rules of Civil Procedure 12(b)(1), 12(b)(2), 12(b)(3), and 12(b)(6) and California's anti-SLAPP statute, California Code of Civil Procedure § 425.16. For the reasons discussed below, the Court concludes that Plaintiff has sufficiently alleged the necessary elements of his claims for under federal and state computer fraud statutes. Defendants' objections raise factual questions that are best addressed in post-discovery briefing. Defendants' Motion is therefore ***denied***.

II. BACKGROUND

The factual allegations center around the appropriation of Plaintiff's data by Defendants. As required by the Federal Rules of Civil Procedure, the following facts are taken from Plaintiff's Complaint [Dkt. No. 1] and are assumed to be true for the purposes of this Motion.

In July 2021, Defendant Ziegler organized Defendant ICU to do business under the name "Marco Polo." Complaint ¶ 20. Defendants then spent at least 13 months — from September 2021 through October 2022 — "analyzing the voluminous material" from Plaintiff's data. *Id.* ¶ 21. Plaintiff is unsure as to how Defendants obtained his data. *Id.* ¶¶ 17–18. Defendant Ziegler used Plaintiff's data to create a lengthy report entitled "Report on the Biden Laptop", which Defendants first published in October 2022. *Id.* ¶ 22. Defendants also used Plaintiff's data to create what Defendant Ziegler described as "an online searchable database of 128,000 emails found on the Biden Laptop." *Id.* Plaintiff never authorized or consented to access of any of his data by any Defendant at any time or for any purpose. *Id.* Plaintiff notified Defendants that they were 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 him immediately. *Id.* ¶ 30. He alleges that Defendants spent multiple months going through the photos stored in his data, organizing and modifying the photos, and subjecting the data to a photo viewing application to allow Defendants and others to view the metadata in the photos. *Id.* ¶ 25.

This application allows those that access Defendants' website to see where the photos were taken, what time they were taken, and other information contained in the metadata. *Id.* Plaintiff also asserts that Ziegler stated that AI tools were needed to censor some of the data. *Id.* ¶ 26.

Plaintiff alleges that Defendants have unlawfully accessed, tampered with, manipulated, damaged, and copied thousands of emails, photos, videos, and recordings, which include financial and bank records. Complaint ¶ 27. He asserts that at least some of the data was originally stored on his iPhone and backed up to his iCloud storage. *Id.* ¶ 28. Plaintiff alleges that Defendants gained unlawful access to his iPhone data by circumventing technical or code-based barriers that were specifically designed and intended to prevent such access. *Id.* While the "precise nature" of how the data was taken and manipulated is unknown, he alleges that the data must be either from Defendants' "copy of the hard drive of the claimed 'Biden laptop' or from Plaintiff's encrypted 'iPhone backup' (or from some other source)." *Id.* ¶ 29.

Plaintiff filed this lawsuit on September 13, 2023, alleging one federal claim for violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, and two state claims for violation of California's Comprehensive Computer Data Access and Fraud Act ("CCDAFA"), Cal. Penal Code § 502, and California's Unfair Competition Law, Business & Professions Code §§ 17200 *et seq.* *See* Complaint. On December 21, 2023, Defendants filed this Motion to dismiss Plaintiff's suit 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.[1]

III. LEGAL STANDARD

Under Rule 12(b)(6), a party may move to dismiss a complaint for failure to state a claim upon which relief may be granted. "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570

[1] On February 29, 2024, Plaintiff filed an opposition ("Opp.") [Dkt. No. 30]. On March 7, 2024, Defendants filed their Reply [Dkt. No. 32]. Defendants also filed Requests for Judicial Notice ("RJN") [Dkt. No. 24], and parties filed a variety of responsive briefings, *see* [Dkt. No. 31, 33, 34]. The Court heard oral argument on May 16, 2024 and took the Motion under submission [Dkt. No. 49].

(2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. Only where a plaintiff fails to "nudge[] [their] claims . . . across the line from conceivable to plausible" is the complaint properly dismissed. *Id*. at 680.

While the plausibility requirement is not a probability assessment, it demands more than "a sheer possibility that a defendant has acted unlawfully." *Id*. at 678. The determination of whether a complaint satisfies the plausibility standard is a "context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *Id*. at 679.

IV. DISCUSSION

A. Subject Matter Jurisdiction And Standing[2]

Defendants initially move to dismiss for lack of subject matter jurisdiction and standing under Rule 12(b)(1) on the ground that Plaintiff "cannot show that any federal statutory violation has occurred" and because Plaintiff "lacks standing" to assert any of his claims. *See* Motion at 4–6.

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, 593 U.S. 374, 379 (2021) (citing 18 U.S.C. § 1030(a)(2)). The CFAA contains a 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)). The CFAA "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 accessor is not entitled so to obtain or alter." *Id.* (citing 18 U.S.C. § 1030(e)(6)). Section 1030(a)(2)'s prohibition initially only applied to certain financial information, but "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)). Thus, "the prohibition now applies—at a

[2] As a preliminary matter, the Court denies Defendants' Request for Judicial Notice of nineteen exhibits. [Dkt. No. 24]. After reviewing the Request, opposition and reply briefing, the Court in its discretion declines to take judicial notice of these exhibits, as none bear on the issues raised in Defendants' Motion.

minimum—to all information from all computers 'used in or affecting interstate or foreign commerce or communication.'" *Id.* (citing 18 U.S.C. § 1030(e)(2)(C, (e)(2)(B)).

Plaintiff's CFFA claim is not "devoid of any merit" as to be wholly insubstantial or frivolous. *See*, *e.g.*, *Custom Packaging Supply, Inc. v. Phillips*, No. 215CV04584ODWAGR, 2015 WL 8334793, at *5 (C.D. Cal. Dec. 7, 2015) (citing *In re Nucorp Energy Sec. Litig.*, 772 F.2d 1486, 1490 (9th Cir. 1985)). Defendants assert that "[n]either the CFAA nor the CCDAFA authorizes a party whose data has been copied to assert a civil action over any computer, device or system not in their possession." Motion at 5. But Defendants fail to point to language in these statutes that require possession of the physical device. Neither the CFAA nor the CCDAFA contain any requirement that Plaintiff must "own," "possess," or "control" the physical device or computer that Defendants accessed. The statute concerns the ownership of the data accessed. Both statutes allow Plaintiff to assert claims based on the facts asserted. *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). In fact, Defendants' ownership-and-control argument has been rejected by the Ninth Circuit. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1078 (9th Cir. 2004) (reversing "district court [that] erred by reading ownership or control requirement into the [CFAA] . . . . Individuals other than the computer's owner may be proximately harmed by unauthorized access, particularly if they have rights to data stored on it.").

Lastly, Defendants attack subject matter jurisdiction on the grounds that Plaintiff's CFAA claim is untimely. But this argument fails because Plaintiff has 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 under 18 U.S.C. § 1030(g). Plaintiff asserts that Defendants spent many months "accessing" and "analyzing" the data, from at least "September 2021 through October 2022." Complaint ¶ 21; *see also* Declaration of Garret Ziegler ("Ziegler Decl.") ¶ 6 [Dkt. No. 23-1]. Plaintiff filed this lawsuit on September 13, 2023, which satisfies the statute of limitations. Most, if not all, of Defendants' acts of unauthorized access to Plaintiff's data occurred within the statute. Thus, the Court has federal question jurisdiction based on Defendants' alleged violation of the

CFAA.[3]

B. Personal Jurisdiction

Defendants contest that the Court has personal jurisdiction over Defendants due to insufficient contacts with California. *See* Motion at 7–12. The plaintiff bears the burden of demonstrating that the court may properly exercise personal jurisdiction over the defendant. *Pebble Beach Co. v. Caddy*, 453 F.3d 1151, 1154 (9th Cir. 2006). To survive a motion to dismiss under Rule 12(b)(2) without an evidentiary hearing, a plaintiff need only make a prima facie showing of jurisdictional facts. *Ballard v. Savage*, 65 F.3d 1495, 1498 (9th Cir. 1995); *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 800 (9th Cir. 2004) ("[W]e only inquire into whether [the plaintiff's] pleadings and affidavits make a prima facie showing of personal jurisdiction.") (citation omitted). "[U]ncontroverted allegations in the complaint must be taken as true." *Id*.

Personal jurisdiction exists if (1) it is permitted by the forum state's long-arm statute and (2) the "exercise of that jurisdiction does not violate federal due process." *Pebble Beach*, 453 F.3d at 1154–55 (citation omitted). California authorizes jurisdiction on any basis consistent with federal due process requirements. Cal. Civ. Proc. Code § 410.10; *Roth v. Garcia Marquez*, 942 F.2d 617, 620 (9th Cir. 1991). The Fourteenth Amendment's Due Process Clause requires that a defendant have "minimum contacts" with the forum state so that the exercise of jurisdiction "does not offend traditional notions of fair play and substantial justice." *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945).

A district court's exercise of personal jurisdiction over a nonresident defendant does not violate due process when the defendant has at least minimum contacts with the forum, and when subjecting the defendant to suit in the forum will "not offend traditional notions of fair play and substantial justice." *See*, *Ayla LLC v. Ayla Skin Pty. Ltd.*, 11 F.4th 972, 979 (9th Cir. 2021) (internal citations omitted).

---

[3] The Court also finds a second basis for subject matter jurisdiction based on diversity jurisdiction under 28 U.S.C. § 1332. *See* Complaint ¶¶ 7–8. Plaintiff is a citizen of the State of California and resides in Los Angeles, California. Defendant Ziegler is a citizen of and is residing in the State of Illinois. Defendant ICU is a corporation organized under the laws of Wyoming. Thus, complete diversity exists between parties. The amount in controversy exceeds $75,000, exclusive of interest and costs, and Plaintiff claims exceed $75,000. *Id.* ¶ 8.

Personal jurisdiction over a nonresident defendant may be general or specific. *Helicopteros Nacionales de Colombia S.A. v. Hall*, 466 U.S. 408, 414–16 (1984). In this case, Plaintiff argues that the Court has specific jurisdiction over Defendant. Opp. at 9–14. A court has specific jurisdiction over a claim that arises out of a defendant's forum-related activities. *Rano v. Sipa Press, Inc.*, 987 F.2d 580, 588 (9th Cir. 1993). To establish specific jurisdiction, the following three-part test must be met:

> (1) The non-resident defendant must purposefully direct his activities or consummate some transaction with the forum or resident thereof; or perform some act by which she purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws; (2) the claim must be one which arises out of or relates to the defendant's forum-related activities; and (3) the exercise of jurisdiction must comport with fair play and substantial justice, i.e. it must be reasonable.

Schwarzenegger, 374 F.3d at 802 (citation omitted). Plaintiff bears the burden of satisfying the first two prongs of the test. *Id.* The burden then shifts to Defendant to "present a compelling case" that the exercise of jurisdiction would not be reasonable. *Id.*

1. Purposeful Direction

Where a plaintiff's claims are based in tort, as they are here, courts use the "purposeful direction" test, 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 Ayala LLC*, 11 F.4th at 979–80 (citing *Calder v. Jones*, 465 U.S. 783 (1984)).[4] Under such a test, courts apply an "effects" test and 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). Even though 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, "whether or not those contacts involve

[4] *See also AMA Multimedia, LLC v. Wanat*, 970 F.3d 1201, 1208 (9th Cir. 2020) (the plaintiff "alleges copyright and trademark infringement claims, which sound in tort, so we apply a 'purposeful direction' analysis and ask whether [the defendant] has purposefully directed activities at the United States").

wrongful activity by the defendant." *Yahoo! Inc.*, 433 F.3d at 1207.[5]

Defendants contest the second prong[6] of the purposeful direction test. More specifically, Defendants contend that Plaintiff can adequately "show that Defendants committed any alleged intentional act that was 'expressly aimed' at California because there was no 'individualized targeting' of California residents by Defendants." Motion at 11. The Court disagrees.

The express aiming inquiry centers on whether the defendant specifically targeted the forum state. *See Morrill v. Scott Fin. Corp.*, 873 F.3d 1136, 1143 (9th Cir. 2017) (citation omitted). The Supreme Court has explained that the contacts supporting purposeful direction "must be the defendant's own choice and not random, isolated or fortuitous." *Ford Motor Co. v. Montana Eighth Jud. Dist. Ct.*, 592 U.S. 351, 359 (2021) (citations omitted). The defendant must have "reached out beyond its home—by, for example, exploiting a market in the forum state." *Id.* (citations omitted). Therefore, a defendant does not purposefully direct its activities at the forum state when the unilateral activity of the plaintiff or a third party is all that connects the defendant to the forum state. *See Walden v. Fiore*, 571 U.S. 277, 284–85 (2014) (citations omitted). Rather, the focus is on the defendant's "own contacts," e.g., "contacts that the defendant *himself* creates with the forum state." *See id.* at 284 (citations omitted) (emphasis in original). "[M]ere injury to a forum resident is not a sufficient connection to the forum." *Id.* at 290. Thus, "[t]he proper question is not where the plaintiff experienced a particular injury or effect but whether the defendant's conduct connects him to the forum in a meaningful way." *Id.* Courts are to focus on the defendant's actual contacts with the forum, and the "quality and nature" of those activities. *Hanson v. Denckla*, 357 U.S. 235, 253 (1958).

Defendant Ziegler notes that the report Defendants prepared using Plaintiff's data is available at the website www.bidenreport.com. Ziegler Decl. ¶ 8 & n.1. On this website, a "Purchase" button

---

[5] Nor is it required that the "brunt" of the harm occurred in the forum state. *Id.* "If a jurisdictionally sufficient amount of harm is suffered in the forum state, it does not matter that even more harm might have been suffered in another state." *Id.*

[6] Defendants do not dispute the first prong that it committed intentional acts by collecting and circulating Plaintiff's data.

is prominently displayed, allowing users to spend $50.00 for a hardcopy of the Biden report. Declaration of Gregory A. Ellis ("Ellis Decl.") ¶ 6, Ex. A [Dkt. No. 30-2]. Clicking the purchase button then links to a purchase page operated by Stripe.com, a California-based entity whose purchase terms are governed by California law.[7] Defendants' argument that this website is purely passive lacks merit. The website, owned and operated by Defendants, allows continuing regular sales from California residents. *C.f. Boschetto v. Hansing*, 539 F.3d 1011, 1018 (9th Cir. 2008) (finding the sale of one item to California resident was insufficient for personal jurisdiction because the "listing temporarily advertised a good for sale and that listing closed once the item was sold, thereby extinguishing the Internet contact for this transaction within the forum state").

Moreover, Defendant Ziegler declares that over six million unique IP addresses have reviewed the report on the Marco Polo website, and that "less than ten percent of Marco Polo's supports reside in California." Ziegler Decl. ¶¶ 12, 16. The question of the exact number of California residents that have purchased the report is unclear, but Ziegler's declaration does not state that no Californians have purchased the physical report. *See* Supplemental Declaration of Garrett Ziegler ("Ziegler's Supp. Decl.") [Dkt. No. 32-1] ¶ 3 ("our supporters can donate funds to secure a hard copy of the Biden Report"). Indeed, with hundreds of thousands of California residents visiting the site, it is more than plausible to assume that California residents have also purchased and continue to purchase a report of Plaintiff's data.[8] Taken together, the Court finds Defendants' statements support targeting into the forum state. The cases cited by Defendants are distinguishable and do not involve a site analogous to that operated by Defendants, which conducts business that allows individuals to purchase copies of the report that compiles Plaintiff's data.[9]

---

[7] *See* www.stripe.com/legal/consumer, Section 12.

[8] The Court need not order further jurisdictional discovery to learn more about the exact details of the financial support from California residents, as the contacts discussed herein are more than sufficient to find specific personal jurisdiction.

[9] *See* Motion at 10–12; *see also Pebble Beach Co. v. Caddy*, 453 F.3d 1151, 1154 (9th Cir. 2006) (defendant hotel's website included only an inquiry form and did not allow visitors to make reservations); *Cybersell, Inc. v. Cybersell, Inc.*, 130 F.3d 414, 419 (9th Cir. 1997) (defendant's

Contacts with the forum are also supported by Ziegler's purported actions after publishing the report to verify the facts and promote the report. For example, he sent copies to multiple California residents to verify Plaintiff's information. Ziegler said in interviews that his team talked with each person named in the report. Ellis Decl. Exs. C at 12 ("I took the time to call each and every person that is in this report") [Dkt. No. 30-5]; D at 8 ("we've sent the dossier to all 4,000 contacts on Hunter's laptop) [Dkt. No. 30-6]. He even includes a table of alleged Plaintiff family crimes with California area codes, many listing "where (venue)" as C.D. Cal. Ellis Decl. Ex. E at 233–35, 400–01. Other California residents include an FBI agent in the San Francisco field office, Ellis Decl. Ex. E at 22. And Ziegler even sent the Report to the personal residence of one of Plaintiff's California-based attorneys. Ellis Decl. ¶ 12.

Ziegler also promoted the Report in California. Ziegler posted a photo of himself holding a copy of the Report in December 2023 on Instagram in front of the Chateau Marmont Hotel in West Hollywood with the caption: "The activities in & around this infamous bungalow are captured for posterity in BidenReport.com." Ellis Decl. Ex. H. He also posted a Rumble video of himself in San Francisco in November 2022, entitled "Report on the Biden Laptop CA Field Trip," again promoting the Report. Ellis Decl. Ex. I. In sum, his entry into California and social media posts reflecting such promotion in California support the exercise of jurisdiction. *See Yue v. Yang*, 62 Cal. App. 5th 539, 543–48 (2021) ("California-focused" social medial messages, including statement that defendant "arrived in California," support specific jurisdiction). Taken together, these contacts with California are more than adequate to satisfy the purposeful direction test.

2. "Arise out of or result from"

Defendants next contest that Plaintiff can show that his claims "arise out of" Defendants' contacts with California. Motion at 11. 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).

---

website only allowed users to email the defendant); *Stomp, Inc. v. NeatO, LLC*, 61 F. Supp. 2d 1074, 1078 (C.D. Cal. 1999) (finding website was not passive where it allowed users to purchase the product at issue).

Ziegler's own statements are sufficient to satisfy the required nexus. In an interview, Ziegler specifically stated that he called "each and every person that is named in this report," which would have included multiple California-based contacts. Ellis Decl. Ex. C. at 13. He tied the credibility of the Report to his verification of the information, tying the manipulation of data at issue to California-based contacts. Further, Plaintiff, a resident of California, is alleged to have suffered harm from Defendants' misuse of his data, supporting this prong. *See Yahoo! Inc.*, 433 F.3d at 1206.

3. Reasonableness

Lastly, Defendants contest personal jurisdiction by arguing that other factors would lead jurisdiction to be unreasonable. Motion at 11–12. This burden is held by Defendants. In evaluating whether jurisdiction would be unreasonable, the Court balances seven factors:

> (1) the extent of the defendants' purposeful interjection into the forum state's affairs; (2) the burden on the defendant of defending in the forum; (3) the extent of conflict with the sovereignty of the defendants' state; (4) the forum state's interest in adjudicating the dispute; (5) the most efficient judicial resolution of the controversy; (6) the importance of the forum to the plaintiff's interest in convenient and effective relief; and (7) the existence of an alternative forum.

Core-Vent Corp. v. Nobel Indus. AB, 11 F.3d 1482, 1487–88 (9th Cir.1993) (citations omitted). But Defendants only address a few factors, claiming that they "did not intentionally target California" and that "the evidence is located in Illinois." Motion at 12. The Court rejects the first argument, as Defendant financially benefitted by accepting purchases of the report by California residents and relied on California residents in creating and promoting the report. The second argument is not enough to tip the scale of reasonableness in their favor, especially considering that Plaintiff lives in California. Balancing the seven factors, the Court finds that jurisdiction is not unreasonable. "California maintains a strong interest in providing an effective means of redress for its residents tortiously injured." *Gordy v. Daily News, L.P.*, 95 F.3d 829, 831, 836 (9th Cir. 1996).

C. Venue

Next, Defendants move to dismiss for lack of venue. Here, facts supporting personal jurisdiction also support venue. "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.'" *United Tactical Sys. LLC v. Real Action Paintball, Inc.*, 108 F. Supp.

3d 733, 751 (N.D. Cal. 2015) (quoting *Decker Coal Co. v. Commonwealth Edison Co.*, 805 F.2d 834, 843 (9th Cir. 1986). Defendant argues that "[w]hile Plaintiff is allegedly a California resident, it is doubtful whether any alleged injuries occurred in California." Motion at 12. But when looking at the entire sequence of events underlying the claim, as Defendants implore the Court to do, *see* Motion at 13, the relevant events include the creation and publication of the website that included Plaintiff's data. These events did not just include Ziegler's decisions but also include California contacts that Ziegler made in developing and publicizing the content of his website and trips to California to promote the report made with Plaintiff's data.

D. Failure to State a Claim

1. CCFA

Plaintiff's first cause of action alleges that 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 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. *See* Motion at 14–17.

Plaintiff's Complaint alleges that Defendants violated the CFAA in various ways, including Section 1030(a)(2)(A) (unauthorized access of records of "financial institution," "card issuer," or "consumer reporting agency"), *see* Complaint ¶ 34; Section 1030(a)(2)(C) (unauthorized access of "information from any protected computer"), *see* Complaint ¶ 35; and Section 1030(a)(4) (unauthorized access of protected computer "knowingly and with intent to defraud" where access furthers the fraud and accessor obtains one or more things of value), *see* Complaint ¶ 36. Plaintiff seeks redress for these violations pursuant to Section 1030(g), which provides that:

> 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 subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

18 U.S.C.A. § 1030(g). Plaintiff alleges that Defendants' conduct involves the factor described in subsection (c)(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." Complaint ¶ 37.

In the Ninth Circuit, the essential elements of a civil claim for violations of Sections 1030(a)(2) and 1030(a)(4) are as follows:

> [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, (2) without authorization or exceeding authorized access, and that he (3) 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.

LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132 (9th Cir. 2009) (citing 18 U.S.C. § 1030(a)).

Applying these statutes to the claims here, the Court finds that Plaintiff has sufficiently alleged each of these elements. *See* Complaint ¶¶ 2, 16–18, 20–22, 24–29 (access); *id.* ¶¶ 4, 17–18, 21–23, 28–30, 34–36 (without authorization); *id.* ¶¶ 22, 24, 27–29 (information obtained); *id.* ¶¶ 2, 16, 18–22, 24–26, 28–29, 35–36 (protected computer); *id.* ¶ 37 (economic "loss" of type recoverable under the statute). Plaintiff's allegations do not merely recite the elements of a CFAA claim; they include sufficient allegations of underlying facts to give fair notice to Defendants.

Defendants' other attacks to the sufficiency of the Complaint fare no better.

First, 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." Motion at 15. But "ownership" and "control" of the physical device is not a required element. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1078 (9th Cir. 2004) (finding that "[t]he 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)").

Second, Defendants argue that it is "questionable whether Plaintiff has adequately alleged that Defendants accessed a 'protected computer'" as defined in the CFAA. *See* Motion at 14. A "protected computer" is "any computer used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). "[T]he term 'computer' means 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…." 18 U.S.C. § 1030(e)(1). This statute's prohibition "now applies—at a minimum—to all information from all computers that connect to the internet." *Van Buren v. United States*, 593 U.S. 374, 379 (2021) (citing §§ 1030(a)(2)(C), (e)(2)(B)). Here, Plaintiffs allege that Defendants accessed a "hard drive" containing Plaintiff's data and created "an online searchable database of 128,000 emails found on the Biden laptop" and public website to house "almost 10,000 photos," and provided the public with metadata and access to password-protected files stored on Plaintiff's iPhone backup. Complaint ¶¶ 22, 24, 25, 29. These allegations are sufficient at this point to allege that Defendants accessed a "computer" that is "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. §§ 1030(e)(1), (e)(2). To go from the hard drive to the public website and database requires internet connectivity, and thus, Plaintiff's allegations are adequate to satisfying this prong.

Third, Defendants claim that "Plaintiff does not allege unlawful access to a computer within the meaning of the CFAA." Motion at 14. But the Complaint contains many factual allegations establishing the unauthorized and unlawful nature of Defendants' data access. Indeed, Plaintiff asserts that Defendants have "accessed" and "analyzed" Plaintiff's data from at least September 2021 until at least October 2022. Complaint ¶ 21. Plaintiff sent a cease-and-desist demand that Defendants did not respond to. *Id.* ¶ 30. Ziegler even admits that with respect to some data, Defendants gained access by circumventing technical barriers. Ziegler Decl. ¶ 21. This is sufficient to allege that Defendants access was authorized and without permission.

Lastly, Defendants argue that Plaintiff has failed to allege a "recoverable loss." Motion at 16–17. The CFAA permits the recovery of losses incurred as a result of investigating and

responding to Defendants' violations of the CFAA. 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 … and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service"). Plaintiff has specifically alleged this, asserting 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." Complaint ¶ 37. That is enough for pleading purposes.

2. CCDAFA

Plaintiff's second cause of action is brought under California's Comprehensive Computer Data Access and Fraud Act, and is codified in California Penal Code § 502. The CCDAFA is broader than CFAA in many respects, and the Court finds that Plaintiff has plead a viable CCDAFA claim. The Complaint alleges violations of California Penal Code Sections 502(c)(1), (c)(2), (c)(3), and (c)(7) of the CCDAFA, which provide that:

> (c) Except as provided in subdivision (h)[10], 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). CCDAFA also contains a private right of action under California Penal Code § 502(e)(1). The CCDAFA is less stringent in its requirements.

> 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

[10] 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).

> takes, copies, or makes use of' data on the computer. Cal. Penal Code § 502(c)(2). A plain reading of the statute demonstrates that its focus is 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) (emphasis in original). The term "access" under the CCDAFA has been defined broadly and "includes logging into a database with a valid password and subsequently taking, copying, or using the information in the database improperly." *Id.*; *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 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." Motion at 17. Not so. The statute specifically refers to "***data*** from a computer," and here Plaintiff plainly asserts a violation of its data by Defendants. Defendants argue that such access was with permission, but Plaintiffs sufficiently contend and allege that they used his passwords to access password-protected files and ignored prelitigation demands to cease and desists.

Defendants also argue that Plaintiff has not suffered damages. That argument fails as well. The CCDAFA provides that 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, damages, or deleted by the access." *Id.* Plaintiff asserts, as the owner of the data, he has suffered damages caused by the Defendant in an amount to be proven in trial. Complaint ¶¶ 39, 44. Plaintiff alleges entitlement to damages, injunctive and other equitable relief. *Id*. ¶¶ 44, 45, 46. Examining Plaintiff's Complaint in its entirety, the Court

finds that damages have been asserted.[11]

E. Anti-SLAPP

Defendants' final argument is that the lawsuit should be dismissed pursuant to California's anti-SLAPP statute. But the anti-SLAPP statute does not apply to federal claims. *See Hilton v. Hallmark Cards*, 599 F.3d 894, 901 (9th Cir. 2010). Thus, Plaintiff's CFAA claim cannot be dismissed on anti-SLAPP grounds.

As for Plaintiff's state law claims, the anti-SLAPP argument lacks merit because Defendants cannot make the prima facie showing that the anti-SLAPP statute requires. *See*, *e.g.*, *Governor Gray Davis Comm. v. Am. Taxpayers Alliance*, 102 Cal. App. 4th 449, 456 (2002) (citations omitted). Defendants must first make an initial prima facie showing that Plaintiff's claims arise from a protected activity. In determining this, "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 burden of the defendants "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").

In this case, Defendants cannot show that Plaintiff's claims "arise from" Defendants' free speech. Defendants argue that their website is a "public forum," that Plaintiff is a "person in the public eye," that this data has been "a topic of widespread, public interest", and that the report of the

[11] Defendants also attack Plaintiff's third cause of action for violation of California's Unfair Competition Law, arguing that it fails because Plaintiff's CFAA and CCDAFA claims are deficient. Motion at 18–19. The Court rejects such arguments, as the CFAA and CCDAFA claims survive.

data that they created and host online has been viewed millions of times. Motion at 21–22. But these assertions do not support the application of the anti-SLAPP statute in this case. Plaintiff did not sue Defendants for creating a report or website. Defendants are being sued for "accessing, tampering with, manipulating, altering, copying and damaging" Plaintiff's computer data. Complaint ¶ 27. Stated differently, the gravamen of the lawsuit is not predicated on protected speech and certainly does not arise from or rely on Defendants' free speech. The anti-SLAPP statute simply 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). Were it otherwise, every data hack of a public figure would be fair game. That is not what California's anti-SLAPP allows.

V. CONCLUSION

For the foregoing reasons, Defendants' Motion is ***denied.***

Dated: June 20, 2024

Hernán D. Vera
United States District Judge