TYLER LAW, LLP
Robert W. Tyler (SBN 179572)
rtyler@tylerlawllp.com
Nathan R. Klein (SBN 306268)
nklein@tylerlawllp.com
Mariah R. Gondeiro (SBN 323683)
mgondeiro@tylerlawllp.com
25026 Las Brisas Road
Murrieta, California 92562
Telephone: (951) 600.2733
Facsimile: (951) 600.4996

Attorneys for Attorneys for Defendants **Garrett Ziegler** and **ICU, LLC**

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

ROBERT HUNTER BIDEN, an individual,

Plaintiff(s)

v.

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

Defendant(s)

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

Honorable Hernan D. Vera
Magistrate Judge Karen L. Stevenson

DEFENDANTS' NOTICE OF MOTION AND 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

Date: February 15, 2024
Time: 10:00 a.m.
Ctrm: 5B

TO EACH PARTY AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on February 15, 2024, at 10:00 a.m., in Courtroom 5B of the above-mentioned courthouse, Defendants Garrett Ziegler and ICU, LLC, a Wyoming limited liability company (collectively "Defendants"), will and hereby move to dismiss Plaintiff Robert Hunter Biden's complaint ("Complaint") in its entirety.

This motion is made following the conference of counsel pursuant to Local Rule 7-3 which took place on Monday, December 11, 2023.

This motion is made 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 and is supported by the concurrently filed memorandum of points and authorities, request for judicial notice and exhibits attached thereto, the [proposed] order, oral argument to be presented at the time of the hearing, and on all other such items the Court may consider.

DATED: December 21, 2023

TYLER LAW, LLP

By: /s/ Robert H. Tyler
Robert H. Tyler, Esq.
Attorneys for Defendants **Garrett Ziegler** and **ICU, LLC**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

I. INTRODUCTION

Plaintiff filed this action in retaliation against Defendants for publishing information, media, and emails originating from the files of the infamous "Biden Laptop." The Plaintiff, a public figure and son of the current U.S. President, abandoned his laptop computer at a Delaware repair shop. The shop owner turned the Biden Laptop over to the FBI on or around October 2019 after discovering disturbing material. Soon after, media outlets gained access to emails and documents found on the Biden Laptop, resulting in a media storm of allegations against Hunter Biden and President Biden regarding potential foreign compromise. By April 2021, Plaintiff appeared in a TV interview discussing the Biden Laptop files found in Delaware and distributed across the internet. Over two years after the dissemination of the Biden Laptop files, Plaintiff inexplicably files this lawsuit against Defendants. Instead of challenging the media outlets, Plaintiff filed half-baked legal challenges against Defendants right before an election season involving his father. Plaintiff's challenges are largely premised on a report Defendants prepared about Hunter Biden as part of their mission of investigating foreign compromise within government. Defendants relied on copies of files from the Biden Laptop that have been widely circulated since the public learned about the Biden Laptop. This Court should dismiss Plaintiff's lawsuit for the following reasons.

First, the Court lacks subject matter jurisdiction because Plaintiff does not state a viable claim under the Computer Fraud and Abuse Act. Plaintiff also lacks standing to bring any claim against Defendants, as he cannot establish a causal connection between Defendants' conduct and his alleged injuries.

Second, Plaintiff cannot establish personal jurisdiction. Defendants do not have the necessary continuous and systematic contacts with California to confer general jurisdiction over it. Plaintiff cannot establish specific jurisdiction either, as Defendants have not purposely directed their activities towards California.

Third, Plaintiff has not stated a claim for relief under the Computer Fraud and

Abuse Act and its analog, the Comprehensive Computer Data and Access Fraud Act. Plaintiff's claim for unfair business practices also fails because it is predicated on the first two causes of action.

Fourth, Plaintiff's lawsuit is subject to an anti-SLAPP. Defendants' conduct constitutes protected activity because it involves a public figure and is a matter of public importance. Plaintiff cannot demonstrate meritorious claims either.

Accordingly, this Court should dismiss the Complaint with prejudice under 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.

II. FACTUAL AND PROCEDURAL BACKGROUND

Plaintiff filed this action on September 13, 2023, alleging that Defendants violated the Computer Fraud and Abuse Act ("CFAA") 18 U.S.C. § 1030(a)(2)(A) and (C) for "intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtaining information," along with a claim under its California analog, the Comprehensive Computer Data and Access Fraud Act ("CCDAFA"), and a claim for unfair business practices. (Complaint ("Compl."), ECF No. 1). Defendants now respond with a motion to dismiss pursuant to Rule 12(b) of the Federal Rules of Civil Procedure and section 425.16 of the California Code of Civil Procedure.

On April 12, 2019, Plaintiff visited a computer repair shop in Wilmington, Delaware, owned by John Paul Mac Isaac, requesting the shop recover information on a laptop computer he dropped off earlier. (RJN, Ex. 1, ¶ 19). The following day, Plaintiff returned to the shop with an external hard drive, requesting Plaintiff transfer the recovered data, as evidenced by a quote sent by Mac Isaac to Plaintiff. (*Id.*, ¶ 20; Ex. 2).

In the process of copying the files, Mac Isaac noticed alarming evidence on Plaintiff's computer and eventually contacted the FBI. (*Id.*, Ex. 4, p. 12). The FBI served Mac Isaac on December 9, 2019 with a Grand Jury Subpoena. (*Id*, Ex. 3). The

electronics remain in possession of the FBI, who analyzed the electronics as part of a criminal investigation that was included in the Congressional testimony of IRS Criminal Supervisory Special Agent Gary A. Shapley, Jr. (*Id.*, Ex. 4, pp. 3, 12-16). Information found on the Biden Laptop is now relevant in a criminal case involving alleged tax crimes by Plaintiff and is pending before this Court. (*Id.*, Ex. 20).

Prior to the FBI taking possession of Plaintiff's damaged laptop and the external hard drive, on or around August 28, 2020, Mac Isaac sent a copy of the laptop data to Robert Costello, an attorney for Rudy Giuliani. (*Id.*, Ex. 1, ¶¶ 26, 28; Ex. 17, ¶¶ 24-26). By October 13, 2020, Plaintiff's attorney, George Mesires, wrote to Mac Isaac asking for the return of the laptop. (*Id.*, Ex. 1, ¶ 31; Ex. 17, ¶ 31). On October 14, 2020, the New York Post published an article about an email found in the Biden Laptop files that suggested that Joe Biden met with Hunter Biden's foreign business partners. (*Id.*, Ex. 6). Thousands of news articles have been published, sourced from countless copies of the data, widely available in the public domain, including a complete duplicate at a publicly accessible website named "MEGA NZ." (Compl. at ¶ 18). MEGA.NZ is a web-based file hosting service operated by MEGA LIMITED, a registered New Zealand Limited Company. (RJN, Exhs. 14-16.)

Despite this extensive dissemination, Plaintiff selectively chose to file a lawsuit against Defendants. More than two years before filing this action, on or around April 4, 2021, Plaintiff appeared in a TV interview discussing a laptop found in Delaware that: included information about him. (*Id.*, Ex. 18). Although Plaintiff asserts "the precise manner by which Defendant Ziegler obtained Plaintiff's data remains unclear", he admits that Jack Maxey, Rudy Giuliani, and MEGA NZ have copies of his Laptop files and further admits these parties are sources of Defendants' copy of the Biden Laptop. (Compl. at ¶¶ 17-18). Plaintiff fails to allege, and cannot allege, that he had any ownership or exclusive right of control over any of the Laptop's files or drives now possessed by third parties. In fact, Plaintiff plainly admits that his data was *first* possessed by third parties, stating that the Laptop's "data appears to

have been tampered with, manipulated, altered and damaged *both before Defendants received it* and after it was obtained by Defendants." (Compl. at ¶ 19 (emphasis added)).

The Complaint lacks specific details about any computer Plaintiff claims Defendants hacked. It mentions an iPhone backup, but a backup is a "copy of files and programs made to facilitate recovery if necessary", not a computer or storage system itself. (Compl. at ¶¶ 40-41; RJN, Ex. 10). Plaintiff accuses Defendants of "knowingly accessing and without permission taking and using data from" Plaintiff's devices or "cloud" storage (Compl. at ¶¶ 40, 41), computer service (*id.* at ¶ 42), or protected computer (*id.* at ¶ 35) but fails to identify a single device Defendants accessed without authorization. The Complaint blithely disregards the publication and possession of the Biden Laptop files, including entities that possessed and circulated the data long before Defendants ever obtained a copy. (RJN, Exhs. 6-8).

Plaintiff selectively cites to Defendant Ziegler's December 2022 remarks about decrypting a specific file which stored the passcode to the iPhone backup file, both of which were on Defendants' copy of the Laptop. (Compl. at ¶ 29). The Complaint falsely suggests Defendants "hacked" into Plaintiff's iPhone backup. (Zeigler Decl. at ¶ 19). Defendants received a copy of Plaintiff's iPhone backup file which existed as part of the files. (*Id.* at ¶ 20). When Defendants received the external hard drive, it contained passcodes, which allowed access to the iPhone backup file. (*Id.* at ¶ 21).

III. ARGUMENT

A. Plaintiff's Lawsuit Is Subject To Dismissal Under Rule 12(b)(1) For Lack Of Subject Matter Jurisdiction.

The Court lacks subject matter jurisdiction because Plaintiff cannot show that any federal statutory violation has occurred. "It is to be presumed that a cause lies outside [of federal courts'] limited jurisdiction, and the burden of establishing the contrary rests upon the party asserting jurisdiction." *Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994) (citations omitted). When determining whether

a claim arises under federal law, a court must "examine the 'well pleaded' allegations of the Complaint and ignore potential defenses: '[A] suit arises under the Constitution and laws of the United States only when the plaintiff's statement of his own cause of action shows that it is based upon those laws or that Constitution.'" *Beneficial Nat'l Bank v. Anderson*, 539 U.S. 1, 6 (2003) (jurisdiction upheld) (quoting *Louisville & Nashville R. Co. v. Mottley*, 211 U.S. 149, 152 (1908) (jurisdiction lacking)). A federal court lacks jurisdiction over a purported claim involving federal law "when the claim is 'so insubstantial, implausible, foreclosed by prior decisions of this Court, or otherwise completely devoid of merit as to not involve a federal controversy.'" *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 89 (1998) (citing *Oneida Indian Nation of N.Y. v. County of Oneida*, 414 U.S. 661, 666 (1974)).

A plaintiff must bring a CFAA action within two years from either: the date of defendant's act or the date plaintiff discovers the unauthorized computer access or damage. 18 U.S.C. § 1030(g). The key inquiry in determining when the limitation period accrues is when the plaintiff learns of the unauthorized access or damage, even if the identity of the perpetrator is unknown. *Sewell v. Bernardin*, 795 F.3d 337, 340 (2d Cir. 2015). The Complaint discloses no violation of the CFAA within the statute of limitations period, and this Court should therefore dismiss this case for lack of subject matter jurisdiction. *See Infra*, at 12-15.

B. Plaintiff's Lawsuit Is Further Subject To Dismissal Under Rule 12(b)(1) For Lack Of Standing.

Neither 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. *See* 18 U.S.C. § 1030(a)(2)(C); Cal. Penal Code § 502(a); *Infra*, at 12-16. Causation of injury must be predicated upon the ability to show a right of ownership and control over the computer, device, or system. *Id.* Without it, Plaintiff lacks standing to maintain an action, as he is not a real party in interest under either statute.

Plaintiff rests the gravamen of his Complaint upon a repeated mantra of

"access," "copying," and "damage" to his computer files in an attempt to persuade the Court that he has suffered a tangible, redressable injury. (Compl. at ¶¶ 16-21, 27-30). Plaintiff lacks standing in this case because, as both Plaintiff's admissions and Defendants' evidence indicate, there is no causal connection between Defendants' conduct and Plaintiff's alleged injuries. Indeed, Plaintiff alleges he is unaware of how the public accessed his data. (*Id.* at ¶¶ 16-21, 27-30).

Additionally, Plaintiff's repeated assertions of lack of knowledge render him unable to plausibly contest the well-documented circumstances that every party in litigation concerning the Laptop have testified in various fora, including investigating law enforcement officials for the U.S. Government. (RJN, Exhs. 4, 6). As described in the facts above, Plaintiff delivered his damaged computer and external hard drive to repairman John Paul Mac Isaac at his shop in Delaware. (*Id.*, Ex. 1, ¶¶ 19-20). Mac Isaac was responsible for transferring the file contents from Plaintiff's computer onto the external hard drive. Mac Isaac has proffered a signed work order invoice that is evidence in a Delaware lawsuit between he and Plaintiff. (*Id.*, Ex. 2).

Plaintiff further admits that Defendants merely possess a copy of the Biden Laptop and that other parties gave copies of the Biden Laptop to Defendants. (Compl. at ¶ 18; Zeigler Decl. at ¶ 5). Plaintiff cannot demonstrate that the device in Defendants' possession ever belonged to him. Absent that ownership right, Plaintiff cannot prove that Defendants caused him any injury under either the CFAA or CCDAFA and, therefore, does not have standing to bring the first two causes of action.

This Court should also dismiss Plaintiff's claim regarding unfair business practices for lack of standing as well. "In determining whether the UCL . . . [applies] to non-California residents, courts consider where the defendant does business, whether the defendant's principal offices are located in California, where class members are located, and the location from which advertising and other promotional literature decisions were made." *Cooper v. Simpson Strong-Tie Company, Inc.*, 460

F. Supp. 3d 894, 911 (N.D. Cal. 2020). The critical issues [ ] are whether the injury occurred in California and whether the conduct of Defendants occurred in California." *Id.* Defendants do not conduct business in California, nor is their principal place of business in California. (Ziegler Decl. at ¶¶ 13-17). Plaintiff cannot establish that his injury transpired in California either. (*Id.* at ¶¶ 5, 17). Plaintiff, therefore, does not have standing to sue under section 17200.

C. Plaintiff's Lawsuit Is Subject To Dismissal Under Rule 12(b)(2) For Lack Of Personal Jurisdiction.

"Where, as here, there is no applicable federal statute governing personal jurisdiction, the law of the state in which the district court sits applies." *Core-Vent Corp. v. Nobel Indus. AB,* 11 F.3d 1482, 1484 (9th Cir.1993) (citation omitted). "California's long-arm statute allows courts to exercise personal jurisdiction over defendants to the extent permitted by the Due Process Clause of the United States Constitution." *Id.* at 1484 (citation omitted). As the United States Supreme Court has long held, the assertion of personal jurisdiction over a nonresident defendant will comport with constitutional due process only if the defendant has sufficient "minimum contacts" with the state such that the maintenance of the suit does not offend "traditional notions of fair play and substantial justice." *International Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945).

1. Defendants Do Not Have the Necessary "Continuous and Systematic Contacts" with California to Confer General Jurisdiction over the State.

This Court lacks general jurisdiction over Defendants under the Supreme Court's decision in *Daimler v. AG Bauer*, 134 S. Ct. 746 (2014). To determine whether general jurisdiction exists, the relevant inquiry is whether "affiliations with the State are so continuous and systematic as to render [it] essentially at home in the forum State." *Id.* at 761 (cleaned up). The Ninth Circuit has held that when determining whether a court's exercise of general jurisdiction over a defendant is

appropriate, "[f]actors to be taken into consideration are whether the defendant makes sales, solicits or engages in business in the state, serves the state's markets, designates an agent for service of process, holds a license, or is incorporated there." *Bancroft & Masters, Inc. v. Augusta Nat'l Inc.*, 223 F.3d 1082, 1086 (9th Cir. 2000).

Defendant Ziegler resides in Illinois. (Compl. at ¶ 12). Defendants hired no employees or independent contractors to conduct business in California, has made no sales in California, and does not have a California agent for service of process or any California license or incorporation. (Ziegler Decl. at ¶ 14). Plaintiff seeks to link Defendants to California through Plaintiffs' operation of a website accessible across the world. (Compl. at ¶ 12). However, the operation of a website does not satisfy the physical presence necessary for general jurisdiction.

Federal courts in California have consistently held that the maintenance of even a highly interactive website, by itself, is not enough to establish general jurisdiction. *Coremetrics, Inc. v. AtomicPark.com*, LLC, 370 F.Supp.2d 1013, 1019-20 (N.D. Cal. 2005). "[I]t is now common for businesses of all types to have an internet website, typically with interactive capability through which customers can communicate with the business and order products. If general jurisdiction were to be predicated on these types of contacts alone, most businesses would be subject to personal jurisdiction in every forum." *Id.* at 1020 (citations omitted); *see also Love v. The Mail on Sunday*, 2006 U.S. Dist. LEXIS 95469, Case No. CV 05-7798 ABC (PJWx) at *11-*12 (C. D. Cal. July 18, 2006) ("[P]ersonal jurisdiction should not be based solely on the ability of forum state residents to access an Internet site within the forum state because that does not by itself show any persistent course of conduct by the defendants.") (citations omitted).

Indeed, courts have declined to exercise general jurisdiction even where the defendant's contact with the forum was more extensive and specific. For example, in *Boaz v. Boyle & Co.*, 40 Cal.App.4th 700, 715-17 (1995), the nonresident defendant's contact consisted of targeting mailers to physicians, advertising principally in national

medical publications, and deriving 9% of its sales from the forum's physicians. The court found that the defendant's level of activity in the forum did not justify the assertion of general jurisdiction. *Id.* at 717-18. Likewise, in *Salu, Inc. v. Original Skin Store*, 2008 WL 3863434, Case No. CIV. S-08- 1035 FCD/KJM, at *3 (E.D. Cal. August 13, 2008), the court refused to exercise general jurisdiction over a website that sold products through an eBay virtual store accessible to consumers across the country. "Plaintiff's contention that 14% of a $50,000 business operation is comprised of sales to California and that business cards are sent in conjunction with delivery of product shipments falls far short of establishing the equivalence of physical presence under the 'exacting standard' required to demonstrate general jurisdiction." *Id.*

Plaintiff claims jurisdiction in California is appropriate because Defendants' website "includes specific disclosures incorporating California consumer protection and privacy laws and purporting to exercise rights under those laws…." (Compl. at ¶ 12). This allegation is woefully inadequate to establish jurisdiction and is not supported by case law.

2. Plaintiff Cannot Satisfy the Three-Part Test for Limited Jurisdiction over Defendants.

The Court may exercise "limited" or "specific" personal jurisdiction if each part of the three prong test is satisfied: (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 he 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 v. Fred Martin Motor Co.*, 374 F.3d 797, 802 (9th Cir. 2004). The plaintiff bears the burden of satisfying the first two prongs of the test. *Id.* If the plaintiff fails to satisfy either of these prongs, personal jurisdiction is not established in the forum state. If the

plaintiff succeeds in satisfying both of the first two prongs, the burden then shifts to the defendant to "present a compelling case" that the exercise of jurisdiction would not be reasonable. *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 476-78 (1985).

First, "[e]vidence of availment is typically action taking place *in* the forum that invokes the benefits and protections of the laws in the forum," whereas "[e]vidence of direction generally consists of action taking place *outside* the forum that is directed at the forum." *Pebble Beach Co. v. Caddy*, 453 F.3d 1151, 1155 (9th Cir. 2006) (emphasis added). Plaintiff does not allege that Defendants took any action from inside California. Rather, Plaintiff alleges that Defendants have taken actions outside California by operating a website that was accessible in California. (Compl. at ¶ 12). Therefore, the purposeful availment test is inapplicable. *Salu*, 2008 WL 3863434 at *4.

Defendants have not purposefully directed their activities toward California either. The purposeful direction test is evaluated under the three-part "effects" test based on *Calder v. Jones*, 465 U.S. 783 (1984). The test "requires that the defendant allegedly have: (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." *Schwarzenegger*, 374 F.3d at 803 (citations omitted). The Plaintiff must show that there was an "individualized targeting" of California residents by the defendant. *Bancroft & Masters, Inc. v. Augusta National, Inc.*, 223 F.3d 1082, 1088 (9th Cir. 2000). For example, in *Pebble Beach Co.*, the court held that the defendant engaged in no "individualized targeting" by registering the domain name "pebblebeach-uk.com" and operating a passive website at that domain, even though he knew that plaintiff resided in the forum. 453 F.3d at 1157. The Court held that the operation of a website that is not expressly aimed at California does not give rise to jurisdiction. *Id.*

In analyzing Internet contacts, the Ninth Circuit has adopted a "sliding scale" approach under which jurisdiction is "directly proportionate to the nature and quality

of commercial activity that an entity conducts over the Internet." *Cybersell, Inc. v. Cybersell, Inc.*, 130 F.3d 414, 419 (9th Cir. 1997). A mere web presence is insufficient to establish jurisdiction. Thus, "passive" websites, which the Ninth Circuit has described as those that merely post information, or on which consumers cannot make purchases, do not give rise to jurisdiction. *Bancroft & Masters*, 223 F.3d at 1086; *Cybersell*, 130 F.3d at 418.

Plaintiff cannot 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. (Ziegler Decl. at ¶ 16). Defendants do not charge users, nor do they engage in for-profit sales of products. (*Id.* at ¶ 15). Defendants' website was passive because it solely existed for "informational purposes." *Stomp, Inc. v. NeatO, LLC*, 61 F.Supp.2d 1074, 1078 (C.D. Cal. 1999).

Second, even if Plaintiff satisfied the first prong, he cannot satisfy the second prong, which requires he show that his claims would not have arisen but for Defendants' contacts with California. *Doe v. American Nat'l Red Cross*, 112 F.3d 1048, 1051 (9th Cir. 1997). Defendants' display of information on their website cannot satisfy this test because the infringement alleged by Plaintiff would have occurred even if Defendants' website was not accessible in California.

Third, even if Plaintiff satisfied the first two prongs, Defendants can defeat jurisdiction by "present[ing] a compelling case that the presence of some other considerations would render jurisdiction unreasonable." *Core-Vent*, 11 F.3d at 1487. Courts balance the following 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.

Id. at 1487-88 (internal citation omitted).

Defendants' contacts with California are attenuated. Defendants did not intentionally target California, nor did the alleged data breaches occur in California. (Ziegler Decl. at ¶¶ 5, 16-17). Litigating this case in Illinois also serves the interests of justice because the evidence is located in Illinois. (*Id.* at ¶ 17). Even if litigating outside the state will inconvenience Plaintiff, neither the Supreme Court nor Ninth Circuit gives much weight to this factor. *Core-Vent*, 11 F.3d at 1490. Plaintiff has not met the burden of proving that he is unable to sue Defendants in Illinois. Thus, the factors tip in Defendants' favor.

D. Plaintiff's Lawsuit Is Subject To Dismissal Under Rule 12(b)(3) For Improper Venue.

Under Federal Rule of Civil Procedure 12(b)(3), a party may file a motion to dismiss for improper venue. *Royal Hawaiian Orchards, L.P. v. Olson*, No. CV 14-8984 RSWL (RZx), 2015 WL 3948821, at *1 (C.D. Cal. June 26, 2015) (citing Fed. R. Civ. P. 12(b)(3)). Plaintiff seeks to establish venue under 28 U.S.C. § 1391(b)(2), which states that venue is proper in the district where "a substantial part of the events or omissions giving rise to the claim occurred." (Compl. at ¶ 9). This substantiality inquiry focuses on the "relevant activities of the defendant, not of the plaintiff." *Woodke v. Dahm*, 70 F.3d 983, 985 (8th Cir. 1995). And "[o]nly the events that directly give rise to a claim are relevant." *Lawler v. Tarallo*, No. C 13-03284 MEJ, 2013 WL 5755685, at *3 (N.D. Cal. Oct. 23, 2013) (simplified). Venue is "intended to preserve the element of fairness so that a defendant is not haled into a remote district having no real relationship to the dispute." *Cottman Transmission Sys., Inc. v. Martino*, 36 F.3d 291, 294 (3d Cir. 1994).

While Plaintiff is allegedly a California resident, it is doubtful whether any alleged injuries occurred in California. Plaintiff has not alleged that any devices from which the alleged data breaches occurred were located in California at the time of the

alleged breaches. Further, Defendants did not obtain copies of Plaintiff's hard drive in California or access his iPhone back-up in California. (Compl. at ¶ 18).

Even if Plaintiff did suffer harm in Los Angeles County, that "is not by itself sufficient to warrant transactional venue there." Wright & Miller, 14D Fed. Prac. & Proc. Juris. § 3806. Otherwise, "venue almost always would be proper at the place of the plaintiff's residence, an option that Congress abolished in the general venue statute." *Id.* Courts thus must look "not to a single triggering event prompting the action, but to the entire sequence of events underlying the claim." *Norsworthy v. Diaz*, 20-CV-01859-JST, 2020 WL 10965424, at *2 (N.D. Cal. June 10, 2020) (simplified).

Applying this standard, Plaintiff's claims did not transpire in this District. Plaintiffs' claims all arise from Defendants' website and publications. At the heart of those claims are Defendant Ziegler's decisions about what content to post on his website. All decision-making occurred in Illinois, the nerve center of operations for ICU and the place where Ziegler resides. (Ziegler Decl. at ¶ 17). Therefore, this Court should dismiss this lawsuit or transfer the case to Illinois. *See Allstar Mktg. Grp., LLC v. Your Store Online, LLC*, 666 F. Supp. 2d 1109, 1126 (C.D. Cal. 2009).

E. Plaintiff's Lawsuit Is Subject To Dismissal Under Rule 12(b)(6) For Failure To State A Claim.

1. Plaintiff's Claim Falls Outside the Statute of Limitations of the Computer Fraud And Abuse Act, 18 U.S.C. § 1030.

As an initial matter, a Plaintiff must bring a CFAA action within two years from either: the date of defendant's act or the date plaintiff discovers the unauthorized computer access or damage. 18 U.S.C. § 1030(g). The key inquiry in determining when the limitation period accrues is when the plaintiff learns of the unauthorized access or damage, even if the identity of the perpetrator is not known. *Sewell*, 795 F.3d at 340. While the precise date when Plaintiff first became aware of access to his data by a third party is presently unknown, it must have indisputably occurred at some date before Plaintiff discussed the contents of his Laptop in a TV interview on or

around April 4, 2021. (RJN, Ex. 18). Plaintiff should have filed this action by April 2023. Therefore, the action should be dismissed with prejudice.

2. Plaintiff Does Not State A Claim under the Computer Fraud And Abuse Act, 18 U.S.C. § 1030.

It is questionable whether Plaintiff has adequately alleged that Defendants accessed a "protected computer" under 18 U.S.C. § 1030(a)(2)(C) and (a)(4). The CFAA defines a computer as "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 definition also includes cellular devices. *See In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 451 (N.D. Cal. 2018) (quoting 18 U.S.C. § 1030(e)(1)-(2)) (holding cellular phones are protected). A "protected computer" under 1030(a)(4) is a computer "which is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). Courts have found this definition to include "any computer connected to the internet, including servers, computers that manage network resources and provide data to other computers." *Miller v. 4Internet*, LLC, 433 F. Supp. 3d 1188, 1198 (D. Nev. 2020). Plaintiff's Laptop and iPhone backup do not satisfy this definition because Plaintiff does not allege that the devices were connected to the Internet when Defendants accessed them.

Moreover, Plaintiff does not allege unlawful access to a computer within the meaning of the CFAA. A computer user "without authorization" is one who accesses a computer the user has no permission to access whatsoever—an "outside hacker[ ]." *Van Buren v. United States*, 141 S. Ct. 1648, 1658, (2021). Here, Plaintiff admitted that Defendants accessed and used a hard drive that Plaintiff never possessed. Specifically, Plaintiff alleges that Defendants accessed a hard drive provided by a third party which contains a copy (duplicates) of files. (Compl. at ¶ 18). Plaintiff does not allege that Defendants possessed or accessed Biden's computer or original files.

Plaintiff alludes to his actual iPhone and iCloud account when he alleges that "at least some of the data that Defendants have accessed, tampered with, manipulated, damaged and copied without Plaintiff's authorization or consent originally was stored on Plaintiff's iPhone and backed-up to Plaintiff's iCloud storage." (*Id.* at ¶ 28). However, Plaintiff alleges no facts which demonstrate Defendants ever accessed any computer, storage, or service which Plaintiff either owns or has exclusive control over. Likewise, the Complaint also shows facts which conclusively prove that Defendants had no need to access any service or storage because the laptop copy in their possession admittedly contained all of the necessary information, including the passcode to view all of the files contained on the Biden Laptop regardless of encryption. (*Id.* at ¶ 18). Put simply, both the encrypted iPhone backup file and the passcode to open the iPhone backup file were on the Laptop copy.

Plaintiff also attempts to conflate use of his data with unauthorized access. In *Van Buren*, the Supreme Court held the following:

> In sum, an individual "exceeds authorized access" when he accesses a computer with authorization but then obtains information located in particular areas of the computer — such as files, folders, or databases — that are off limits to him. The parties agree that Van Buren accessed the law enforcement database system with authorization.

141 S. Ct. at 1662.

This holding demonstrates that use of data from a computer is immaterial in determining liability. The Ninth Circuit expressed concern about broadening the scope of the CFAA in *U.S. v. Nosal*, as doing so would "transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." 676 F.3d 854, 857 (9th Cir. 2012).

Plaintiff invites the Court to speculate as to wrongdoing on the Defendants' part – while blithely ignoring that many acknowledged copies of Plaintiff's Laptop exist, and contents have been published by other parties. (RJN, Ex. 6). Plaintiff's

"[t]hreadbare recitals of the elements of [the CFAA], supported by merely conclusory statements, do not suffice." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal citation omitted).

Finally, Biden does not allege any recoverable "loss." The CFAA defines "loss" to include: (1) "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 (2) "any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11); *see Brown Jordan v. Carmicle*, 846 F.3d 1167, 1174 (11th Cir. 2017) (finding that either or both categories may suffice). Furthermore, the "loss" must amount to at least $5,000 in a one-year period. 18 U.S.C. § 1030(c)(a)(4)(A)(i)(I).

Provisions defining "damage" and "loss" specify what a plaintiff in a civil suit can recover. "[D]amage" means "any impairment to the integrity or availability of data, a program, a system, or information." *Id.* § 1030(e)(8). The term "loss" likewise relates to costs caused by harm to computer data, programs, systems, or information services. *Id.* § 1030(e)(11). The statutory definitions of "damage" and "loss" focus on technological harms – such as the corruption of files – of the type of unauthorized users cause to computer systems and data. Limiting "damage" and "loss" in this way makes sense in a scheme "aimed at preventing the typical consequences of hacking." *Royal Truck & Trailer Sales & Serv., Inc. v. Kraft*, 974 F.3d 756, 762 (6th Cir. 2020). The term's definitions are unsuitable, however, to remediate "misuse" of sensitive information that an individual permissibly accesses using their computers. *Ibid.*

Here, Plaintiff primarily alleges he incurred loss as a result of "investigating and responding to Defendants' violations of the CFAA". (Compl. at ¶ 37). But the CFAA does not provide for recovery of legal expenses, lost profits, or other consequential damages untethered to a service interruption or restoration and/or response effort. *See* 18 U.S.C. 1030(e)(11). The CFAA prohibits unauthorized access

to a computer, not misuse of information obtained therefrom. *See Van Buren*, 141 S. Ct. at 1659–60. Plaintiff's single reference to "direct costs, incurred during any one-year period, of investigating and responding to Defendants' violations of the CFAA" is conclusory and unsupported by any factual allegations. (Compl. at ¶ 37). This Court should therefore dismiss Plaintiff's CFAA claim because he does not allege recoverable damages.

3. Plaintiff Does Not State A Claim under the Comprehensive Computer Data Access and Fraud Act.

The CCDAFA, codified in California Penal Code § 502, is intended to protect individuals from "from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a). The CCDAFA is analogous to the CFAA in that it requires a defendant to access a computer or device belonging to, or controlled by, the Plaintiff. As stated in CACI No. 1812. Comprehensive Computer Data and Access Fraud Act - Essential Factual Elements (Pen. Code, § 502), Plaintiff's Complaint specifically requires a showing of ownership and control of the accessed computer as a prerequisite of liability. Judicial Council of California Civil Jury Instructions (2023).

Plaintiff does not present any facts that Defendants acted "without permission." (Compl. at ¶ 40). As the CCDAFA jury instruction indicates, ownership of the hard drive in Defendants' possession would be a necessary prerequisite to assert the right to grant or deny permission to the Defendants in order to access the files it contains. Defendants did not possess or access Plaintiff's computer or devices, let alone his original files; the Defendants, again, only possess duplicates as Plaintiff admits. And Plaintiff has not asserted (and logically cannot assert) that he ever owned or exercised any right of control over the hard drive possessed by Defendants.

Moreover, Plaintiff does not allege that he suffered damages. Section 502 "permits 'the owner or lessee' of the computer or data 'who suffers damage or loss by reason of a violation' to bring a civil action." *Mintz v. Mark Bartelstein & Assoc.*

Inc., 906 F. Supp. 2d 1017, 1031 (C.D. Cal. 2012); Cal. Penal Code § 502(e)(1). The Complaint does not demonstrate what actions, if any, Plaintiff did to prevent any alleged violations of section 502. The Complaint alleges that Plaintiff "notified Defendants that Defendants 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 in their possession to Plaintiff immediately." (Compl. at ¶ 22). This assertion is meaningless and proves no damages under the CCDAFA.

In sum, the Complaint is merely an invitation to speculate and is nothing more than an attempt to use the CFAA and CCDAFA as a meritless surrogate for a deficient misappropriate claim. The Complaint states formulaic and conclusory conjecture, rather than setting forth a plain statement of facts describing actions or events giving rise to a claim under the CFAA and CCDAFA.

4. Plaintiff Does Not State A Claim for Unfair Businesses Practices under California Business and Professions Code § 17200.

"To state a claim for unfair business practices, plaintiff . . . must allege that defendant . . . engaged in business conduct that was unfair, unlawful or fraudulent." Cal. Bus. & Prof. Code § 17200. Regarding the "unfairness" prong, "there is some uncertainty about the appropriate definition of the word 'unfair' in consumer cases brought under section 17200." *Camacho v. Automobile Club of Southern California*, 142 Cal.App.4th 1394, 1400 (2006). "When a plaintiff who claims to have suffered injury from a direct competitor's 'unfair' act or practice invokes section 17200, the word 'unfair' in that section means conduct that threatens an incipient violation of an antitrust law, or violates the policy or spirit of one of those laws because its effects are comparable to or the same as a violation of the law, or otherwise significantly threatens or harms competition." *Cel–Tech Communications, Inc. v. Los Angeles Cellular Telephone Co*., 20 Cal.4th 163, 187 (1999).

Here, Plaintiff has not alleged that Defendants' actions were unfair to consumers or violative of anti-trust laws. Plaintiff claims Defendants violated section

17200 because they "have engaged in unfair and unlawful activities in violation of the CFAA and California Penal Code section 502." (Compl. at ¶ 22). Because Plaintiff does not state a claim for relief regarding his first two causes of action, this Court should dismiss the third cause of action.

F. Plaintiff's Lawsuit Is Subject To Dismissal Under Rule 12(b)(6) And California Code Of Civil Procedure § 425.16.

Additionally, the Court should note that Plaintiff's action is, quintessentially, a SLAPP action. California Code of Civil Procedure § 425.16 allows a defendant to dismiss an action aimed at chilling the valid exercise of the constitutional rights of freedom of speech and petition for redress of grievances. "[T]he conceptual features which reveal themselves as SLAPP's are that they are generally meritless suits brought by large private interests to deter common citizens from exercising their political or legal rights or to punish them for doing so." *Wilcox v. Superior Court*, 27 Cal. App. 4th 809, 815-17 (1994). Stated another way, "SLAPP suits are brought to obtain an economic advantage over the defendant, not to vindicate a legally cognizable right of the plaintiff." *Id.* at 816. "A Court considering a motion to strike under the anti-SLAPP statute must engage in a two-part inquiry. First, a defendant must make an initial prima facie showing that the plaintiff's suit arises from an act in furtherance of the defendant's rights of petition or free speech.…. Second, once the defendant has made a prima facia showing, the burden shifts to the plaintiff to demonstrate a probability of prevailing on the challenged claims." *Pac. Surrogacy U.S., L.L.C. v. Bai*, No. SA CV 19-01456-DOC (JDEx), 2019 WL 8129615, at *6 (C.D. Cal. Nov. 5, 2019) (internal citation omitted).

In determining whether Defendants have sustained their initial burden, the Court shall consider the pleadings, declarations, and matters that may be judicially noticed. *Brill Media Co., LLC v. TCW Group, Inc.*, 132 Cal. App. 4th 324, 339 (2005). Defendants need not show that Plaintiff's lawsuit was brought with the subjective intent to "chill" their rights of petition and free speech. *Equilon Enterprises, LLC v.*

Consumer Cause, Inc., 29 Cal. 4th 53, 58 (2002). Moreover, Defendants need not demonstrate that Plaintiff's Complaint actually had a "chilling" effect. *Id.* at 59.

1. Defendants' Speech Constitutes Protected Activity

At the first step, Defendants can demonstrate that their speech encompasses the "right of petition or free speech under the United States Constitution or the California Constitution in connection with a public issue... " Cal. Code Civ. Proc.§ 425.16(b)(l). Sections 425.16(e)(3) and (4) of the anti-SLAPP statute protects speech or non-speech conduct made or done "in connection with a public issue or an issue of public interest." To determine whether speech or non-speech conduct is "in connection with" an issue of public interest, a court must consider both the context and the content of the statements or non-speech conduct at issue through a two-part process. *FilmOn.com Inc. v. DoubleVerify Inc.*, 7 Cal. 5th 133, 149 (2019). Under the *FilmOn* analysis, first, "the court is to examine what 'public issue or … issue of public interest' the speech in question implicates." *Id.* In this step, the court examines the content of the speech." *Id.* In the second step, the court examines the functional relationship between speech and the public conversation about the matters of public interest implicated. *Id.* at 149-50. In this step, the court examines the context of the speech or non-speech conduct. *Id.* at 150.

The speech and non-speech conduct at issue in the Complaint were made in connection with an issue of public interest. As discussed below, Defendants satisfy both the "public issue" step and the "functional relationship" step.

a. *The speech and conduct at issue in the Complaint were made or done in connection with a public issue or an issue of public interest.*

First, an "issue of public interest" has been defined using three categories: (1) a person or entity in the public eye; (2) conduct that could directly affect a large number of people beyond the direct participants; or (3) a topic of widespread, public interest. *See Rivero v. American Federation of State, County, and Municipal Employees, AFL-CIO*, 105 Cal. App. 4th 913, 924 (2003). "A 'public forum' is

traditionally defined as a place that is open to the public where information is freely exchanged." *Damon v. Ocean Hills Journalism Club*, 85 Cal. App. 4th 468,475 (2000), citing *Clark v. Burleigh*, 4 Cal. 4th 474, 482 (1992). "In articulating what constitutes a matter of public interest, courts look to certain specific considerations, such as whether the subject of the speech or activity was a person or entity in the public eye or could affect large numbers of people beyond the direct participants; and whether the activity occurred in the context of an ongoing controversy, dispute or discussion or affected a community in a manner similar to that of a governmental entity." *FilmOn*, 7 Cal.5th at 145-46. "The right to speak on political matters is the quintessential subject of our constitutional protections of the right of free speech." *Matson v. Dvorak*, 40 Cal. App. 4th 539, 548 (1995).

Defendants' website is a public forum because it is open to the public and free of charge. Courts have repeatedly held that websites that circulate newsworthy materials are public forums. *See Barrett v. Rosenthal*, 40 Cal.4th 33, 41 n. 4 (2006) ("Web sites accessible to the public, like ... 'newsgroups' ... are 'public forums' for purposes of the anti-SLAPP statute."); *see also Wong v. Tai Jing*, 189 Cal.App.4th 1354, 1366 (2010) ("It is settled that 'Web sites accessible to the public ... are public forums for purposes of the anti-SLAPP statute.' ").

The public is entitled to Defendants' comments and reports about Plaintiff Hunter Biden because they implicate President Joe Biden's "character and fitness for public office…." *Vogel v. Felice*, 127 Cal. App. 4th 1006, 1015-16 (2005) (collecting cases). Hunter Biden is undoubtedly a person in the public eye. The Biden Laptop has been "a topic of widespread, public interest" since at least October 14, 2020, when the New York Post published an article entitled, "Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad." (RJN, Ex. 6). The Biden Laptop was still the subject of public discussion in 2022. Thousands of news articles have been published regarding the Biden Laptop. (Compl. at ¶ 22; Ziegler Decl. at ¶¶ 10-11).

Second, in addressing the context of the speech under the "functional test," the *FilmOn* Court emphasized that it does not look to the substance of the speech or its social utility, by stating:

> our inquiry does not turn on a normative evaluation of the substance of the speech. We are not concerned with the social utility of the speech at issue, or the degree to which it propelled the conversation in any particular direction; rather, we examine whether a defendant—through public or private speech or conduct–participated in, or furthered, the discourse that makes an issue one of public interest.

7 Cal.5th at 151. "It is at the latter stage that context proves useful." *Id.* at 150.

Here, Defendants participated in the discourse that makes the Biden Laptop an issue of public interest. Defendant Ziegler created a voluminous report detailing potential violations of state and federal law. (Zeigler Decl. at ¶¶ 6-8). He also created a website to house thousands of photos and emails from the Biden Laptop and shared this information with members of the media and on social media. (*Id.* at ¶¶ 8-10). Defendants' conduct required significant "newsgathering, which therefore can be constructed as undertaken in furtherance of the news media's right to free speech." *Lieberman v. KCOP Television, Inc.*, 110 Cal. App. 4th 156, 166 (2003). Indeed, mainstream media has cited Defendants' report over 300 times. (Ziegler Decl. at ¶ 10). More than six million unique IP addresses have reviewed the report on Defendants' website. (*Id.* at ¶ 12). Consequently, the speech and conduct at issue in this case satisfies the second test under the *FilmOn* inquiry.

2. Plaintiff Does Not Have A Probability of Prevailing on the Merits

At the second step, the burden shifts to Plaintiff to demonstrate "a probability that [he] will prevail" on the merits. Cal. Code Civ. Proc. § 425.l 6(b)(l). Defendants will not prevail on the merits for the following reasons.

First, a computer user "without authorization" is one who accesses a computer the user has no permission to access whatsoever—an "outside hacker[ ]." *Van Buren*,

141 S. Ct. at 1658. As a threshold matter, Plaintiff's CFAA claim fails because he did not raise the claim within the statute of limitations, rendering the entire lawsuit illegitimate for lack of subject matter jurisdiction. (RJN, Ex. 18). Defendants did not possess or access Biden's computer or original files. (Ziegler Decl. at ¶ 5). No person associated with Marco Polo has "accessed or attempted to access any computer, device, service, or system owned or controlled by Plaintiff." (*Id.* at ¶ 22). Plaintiff cannot demonstrate that he had dominion or control over the devices in the Defendants' possession. Plaintiff, therefore, will not prevail on the merits of his CFAA claim.

Second, and for related reasons, Plaintiff's CCDAFA claim is meritless because Plaintiff does not present any facts that Defendants acted without permission. Defendants, again, only accessed duplicate files, and never hacked into Plaintiff's backup. (*Id.* at ¶¶ 5, 19-22). Defendants' report on the Biden Laptop concerns the materials found in Defendants' copy of Plaintiff's duplicated files. (*Id.* at ¶ 23). As explained above, Plaintiff did not suffer damages under the CCDAFA. *See Supra*, at 17-18. Thus, Plaintiff's CCDAFA claim is untenable.

Third, Plaintiff will not prevail on his unfair business practices claim because it hinges on the first two causes of action, which are devoid of merit. Plaintiff cannot demonstrate that Defendants' actions were unfair to consumers or violated anti-trust laws either.

In sum, Defendants have demonstrated that their conduct is a protected activity because it involves a matter of significant public interest. Plaintiff cannot satisfy his burden of demonstrating meritorious claims. This lawsuit is therefore subject to anti-SLAPP.

IV. CONCLUSION

Considering the foregoing, this Court should dismiss the Complaint with prejudice under 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.

DATED: December 21, 2023

TYLER LAW, LLP

By: /s/ Robert H. Tyler
Robert H. Tyler, Esq.
Attorneys for Defendants **Garrett Ziegler** and **ICU, LLC**