

1 PAUL B. SALVATY (State Bar No. 171507)
PSalvaty@winston.com
2 WINSTON & STRAWN LLP
333 S. Grand Ave., 38th Fl.
3 Los Angeles, CA 90071-1543
Telephone: (213) 615-1700
4 Facsimile: (213) 615-1750

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

9 BRYAN M. SULLIVAN (State Bar No. 209743)
bsullivan@earlysullivan.com
10 ZACHARY C. HANSEN (State Bar No. 325128)
zhansen@earlysullivan.com
11 EARLY SULLIVAN WRIGHT GIZER & McRAE LLP
6420 Wilshire Boulevard, 17th Fl.
12 Los Angeles, California 90048
Telephone: (323) 301-4660
13 Facsimile: (323) 301-4676

14 Attorneys for Plaintiff
ROBERT HUNTER BIDEN

15
16 **UNITED STATES DISTRICT COURT**
17 **CENTRAL DISTRICT OF CALIFORNIA**

18 ROBERT HUNTER BIDEN, an
19 individual,

20 Plaintiff,

21 vs.

22 GARRETT ZIEGLER, an individual,
23 ICU, LLC, a Wyoming Limited Liability
24 Company d/b/a Marco Polo, and DOES
1 through 10, inclusive;

25 Defendants.
26
27
28

Case No. 2:23-cv-07593

**COMPLAINT FOR DAMAGES,
INJUNCTIVE AND EQUITABLE
RELIEF:**

1. **VIOLATION OF THE
COMPUTER FRAUD AND
ABUSE ACT (18 U.S.C. § 1030)**
2. **VIOLATION OF THE
CALIFORNIA COMPUTER
DATA ACCESS AND FRAUD
ACT (CAL. PENAL CODE
§ 502)**
3. **BUS. & PROF. CODE
SECTIONS 17200 *et seq.***

DEMAND FOR JURY TRIAL

1 Plaintiff Robert Hunter Biden (“Plaintiff”), for his claims against Defendant
2 Garrett Ziegler (“Ziegler”) and Defendant ICU LLC (“ICU”) (collectively,
3 “Defendants”) alleges upon knowledge with respect to his own acts and upon
4 information and belief as to all other matters, as follows:

5 **INTRODUCTION**

6 1. Garrett Ziegler is a zealot who has waged a sustained, unhinged and
7 obsessed campaign against Plaintiff and the entire Biden family for more than two
8 years. While Defendant Ziegler is entitled to his extremist and counterfactual opinions,
9 he has no right to engage in illegal activities to advance his right-wing agenda. Yet that
10 is precisely what Defendant Ziegler and his so-called “nonprofit research group,”
11 Defendant ICU, d/b/a/ Marco Polo, have done and have asserted they will continue to
12 do in the future.

13 2. Since approximately December 2020, Defendant Ziegler, Defendant ICU
14 and their “team” of volunteers and independent contractors have spent countless hours
15 accessing, tampering with, manipulating, altering, copying and damaging computer
16 data that they do not own and that they claim to have obtained from hacking into
17 Plaintiff’s iPhone data and from scouring a copy of the hard drive of what they claim
18 to be Plaintiff’s “laptop” computer.

19 3. Defendants’ actions are unlawful under the Computer Fraud and Abuse
20 Act (18 U.S.C. § 1030), California’s Computer Data Access and Fraud Act (Cal. Penal
21 Code § 502) and California’s Unfair Competition Law (Cal. Bus. & Prof. Code §§
22 17200 *et seq.*).

23 4. Plaintiff has demanded Defendants cease their unlawful activities with
24 respect to Plaintiff’s data and return any data in their possession belonging to Plaintiff,
25 but they have flatly and publicly refused to do so. Rather than comply, Defendants
26 have doubled down on their illegal actions and have vowed to continue violating the
27 law with impunity, thereby necessitating this action.
28

1 N. Gould Street, Ste 12323, Sheridan, WY 82801. Plaintiff is further informed and
2 believes that Defendant Ziegler serves as an officer, manager or director of Defendant
3 ICU and is primarily responsible for the management of Defendant ICU. Plaintiff is
4 further informed and believes that Defendant ICU engages in regular activities in
5 California and the County of Los Angeles, including, among other actions, operating a
6 website which includes specific disclosures incorporating California consumer
7 protection and privacy laws and purporting to exercise rights under those laws,
8 demonstrating that Defendants directed their actions to California and purposely
9 availed themselves of California law.

10 13. Defendants sued herein as Does 1 through 10, inclusive, are sued in their
11 fictitious names and capacities as their identities have not yet been determined.
12 Plaintiff is informed and believes and thereon alleges that each of such Defendants is
13 responsible in some way for the acts alleged herein. Plaintiff will seek leave to amend
14 this complaint to allege such Defendants' true names and capacities when they have
15 been ascertained.

16 14. Upon information and belief, at all times herein mentioned, each
17 Defendant acted individually and/or as the agent, co-conspirator, aider, abettor, joint
18 venturer, alter ego, third-party beneficiary, employee, officer, director or representative
19 of the other Defendants and, in doing the things hereinafter averred, acted within the
20 course and scope of such agency, employment or conspiracy and with the consent,
21 permission and authorization of each of the remaining Defendants. Upon information
22 and belief, all actions of each Defendant as averred in the claims for relief stated herein
23 were ratified and approved by every other Defendant or their officers, directors or
24 managing agents.

25 **FACTUAL ALLEGATIONS**

26 15. Defendant Ziegler is a former Trump White House aide who worked, from
27 February 2019 until January 2021, as a Policy Analyst and, later, as an Associate
28 Director of the Office of Trade and Manufacturing Policy under the supervision of Dr.

1 Peter Navarro.

2 16. Plaintiff is informed and believes and thereon alleges that, since having
3 his White House credentials revoked by former White House Chief of Staff Mark
4 Meadows in or around January 2021, Defendant Ziegler has devoted most of his waking
5 time and energy to accessing, tampering with, manipulating, altering, copying and
6 otherwise using data contained on a copy of a hard drive that Defendants claim to be
7 of Plaintiff's "laptop" computer and data that Defendants admit to have obtained by
8 hacking into Plaintiff's data, specifically an encrypted iPhone backup.

9 17. Although the precise manner by which Defendant Ziegler obtained
10 Plaintiff's data remains unclear, there is no dispute that Defendants have, to at least
11 some extent, accessed, tampered with, manipulated, altered, copied and damaged
12 Plaintiff's data, and that their actions are illegal, unauthorized, and without Plaintiff's
13 consent.

14 18. According to published reports, Defendant Ziegler claims to have obtained
15 one copy of a hard drive from what he claims was Plaintiff's "laptop" computer in
16 December 2020 from Jack Maxey, a former co-host on Steve Bannon's *War Room*
17 podcast who has described himself publicly as "Hunter's Laptop King." In or around
18 early 2021, Defendant Ziegler claims to have obtained another copy of a hard drive
19 from what he claims to be Plaintiff's "laptop" computer from an associate of Rudy
20 Giuliani, the former New York mayor who previously represented former President
21 Trump. Plaintiff is informed and believes and thereon alleges that Defendant Ziegler
22 also illegally accessed, tampered with, manipulated and copied data belonging to
23 Plaintiff by means of a "cloud" storage and file hosting service offered by MEGA NZ.

24 19. Plaintiff's data appears to have been tampered with, manipulated, altered
25 and damaged both before Defendants received it and after it was obtained by
26 Defendants and they began illegally accessing and tampering with it themselves.
27 Plaintiff is informed and believes and thereon alleges that Defendants intentionally
28 altered at least some of Plaintiff's data and that they severely damaged Plaintiff's data

1 through sloppy and inept handling of the data, by disregarding forensically sound
2 methods for data preservation and analysis, and by engaging generally in reckless,
3 incompetent and malicious activities with respect to the data that have impaired the
4 ability of Plaintiff and others to verify all of the data's authenticity and to determine the
5 precise extent of tampering, alteration and damage.

6 20. On or about July 8, 2021, Defendant Ziegler organized Defendant ICU and
7 caused Defendant ICU to begin doing business under the name *Marco Polo*. According
8 to Defendant Ziegler's own public statements, a chief focus of Defendant ICU has been
9 accessing and analyzing Plaintiff's data. In addition to illegally accessing and
10 analyzing the data, Defendants also have tampered with, manipulated and copied the
11 data so that others could unlawfully access, tamper with and manipulate Plaintiff's data
12 as well.

13 21. Plaintiff is unaware of the precise dates on which Defendants have
14 accessed, altered, tampered with, manipulated, damaged and/or copied Plaintiff's data.
15 According to Defendant Ziegler himself, Defendants spent at least 13 months – from
16 September 2021 through October 2022 – “analyzing the voluminous material from the
17 Biden Laptop.” On information and belief, Defendants' unlawful access, tampering
18 with, manipulation, damage and copying of Plaintiff's data has continued beyond
19 October 2022 and is ongoing to this day.

20 22. Defendant Ziegler has stated publicly that Defendants used Plaintiff's data
21 from what he calls Plaintiff's “laptop” computer to create a voluminous report entitled
22 *Report on the Biden Laptop*, which Defendants first published on or about October 19,
23 2022. In addition, in or around May 2022, Defendants used Plaintiff's data from the
24 claimed Plaintiff's “laptop” computer to create what Defendant Ziegler has described
25 as “an online searchable database of 128,000 emails found on the Biden Laptop.”
26 Plaintiff has never authorized or consented to any access of his data by any Defendant
27 (or anyone working with any Defendant) at any time or for any purpose. To the
28 contrary, Plaintiff has notified Defendants that Defendants are not authorized to access

1 any of his data, that they should cease doing so, and that they should return any of
2 Plaintiff's data in their possession to Plaintiff immediately.

3 23. Defendants not only admit to accessing, tampering with, manipulating and
4 copying Plaintiff's data from their claimed Plaintiff's "laptop" computer without
5 Plaintiff's authorization or consent, they regularly brag about their illegal activities in
6 interviews with members of the media, on social media, and on right-wing podcasts.

7 24. For example, in December 2022, Defendant Ziegler described the
8 activities of his team, which he said includes "digital forensics folks," as follows: "[I]t
9 took us a year to go through [the data] . . . Usually, when you have this much data to
10 go through, it's as if it's after a presidential library has been opened, right?" In another
11 interview published in or around June 2023, Defendant Ziegler discussed his and his
12 team's efforts to create a website to house "almost 10,000 photos" that he claims to
13 have extracted from Plaintiff's data.

14 25. According to Defendant Ziegler, Defendants spent "a couple of months"
15 going through photos stored in Plaintiff's data, organizing and modifying the photos
16 (through what he characterizes as "redactions"), and subjecting the data to a "photo
17 viewing app" to allow Defendants and others to "view the metadata in the photos."
18 Defendant Ziegler claims that Defendants' activities are designed to allow members of
19 the public who log onto Defendants' website and access Defendants' servers "to be
20 able to see where the photo was taken, what time it was taken, if it has latitude and
21 longitude coordinates attached to it. . . They're going to be able to see if it has metadata
22 like aperture, lighting."

23 26. Defendant Ziegler further has stated that Defendants' efforts to upload
24 videos from Plaintiff's data to Defendants' website required more time and effort than
25 uploading photos from Plaintiff's data because Defendants needed "to use AI tools" on
26 the data as part of their purported efforts to "censor" portions of videos that Defendants
27 consider to be "pornographic."

28 27. Plaintiff is informed and believes and thereon alleges that the data

1 Defendants have accessed, tampered with, manipulated, damaged and copied includes
2 tens of thousands of emails, thousands of photos, and dozens of videos and recordings.
3 Plaintiff is informed and believes and thereon alleges that the data Defendants have
4 accessed, tampered with, manipulated and copied also includes Plaintiff's credit card
5 details, Plaintiff's financial and bank records, and information of the type contained in
6 a file of a consumer reporting agency.

7 28. Plaintiff further is informed and believes and thereon alleges that at least
8 some of the data that Defendants have accessed, tampered with, manipulated, damaged
9 and copied without Plaintiff's authorization or consent originally was stored on
10 Plaintiff's iPhone and backed-up to Plaintiff's iCloud storage. On information and
11 belief, Defendants gained their unlawful access to Plaintiff's iPhone data by
12 circumventing technical or code-based barriers that were specifically designed and
13 intended to prevent such access.

14 29. In an interview that occurred in or around December 2022, Defendant
15 Ziegler bragged that Defendants had hacked their way into data purportedly stored on
16 or originating from Plaintiff's iPhone: "And we actually got into [Plaintiff's] iPhone
17 backup, we were the first group to do it in June of 2022, we cracked the encrypted code
18 that was stored on his laptop." After "cracking the encrypted code that was stored on
19 [Plaintiff's] laptop," Defendants illegally accessed the data from the iPhone backup,
20 and then uploaded Plaintiff's encrypted iPhone data to their website, where it remains
21 accessible to this day. It appears that data that Defendants have uploaded to their
22 website from Plaintiff's encrypted "iPhone backup," like data that Defendants have
23 uploaded from their copy of the hard drive of the "Biden laptop," has been manipulated,
24 tampered with, altered and/or damaged by Defendants. The precise nature and extent
25 of Defendants' manipulation, tampering, alteration, damage and copying of Plaintiff's
26 data, either from their copy of the hard drive of the claimed "Biden laptop" or from
27 Plaintiff's encrypted "iPhone backup" (or from some other source), is unknown to
28 Plaintiff due to Defendants' continuing refusal to return the data to Plaintiff so that it

1 can be analyzed or inspected.

2 30. Plaintiff has demanded that Defendants cease and desist from their
3 unlawful accessing of Plaintiff's data and that they return any data in their possession
4 that was sent to them or that they obtained from any account, device/hard drive, back
5 up files, "cloud" files or copies of the same belonging to Plaintiff. Rather than comply,
6 Defendants have derided Plaintiff and Plaintiff's counsel for making the demands, and
7 they have vowed to continue violating the law with impunity.

8 31. Within the last two weeks, Defendant Ziegler went so far as to declare on
9 social media that efforts by Plaintiff to serve him with legal process in the future would
10 met with violence: "If the US pResident's son sends a proxy [*i.e.*, a process server] to
11 illegally trespass on my property I will blow their f---ing brains out."

12 32. In light of the foregoing illegal activities by Defendants, their repeated
13 refusals to cease and desist in their unlawful behavior, and their stated intention to
14 continue violating the law in the future, Plaintiff has no alternative but to commence
15 this lawsuit and to seek all available and appropriate legal and equitable relief.

16 **FIRST CLAIM FOR RELIEF**

17 **(Violation of the Computer Fraud and Abuse Act)**

18 **(18 U.S.C. § 1030)**

19 **(Against all Defendants)**

20 33. Plaintiff incorporates herein by this reference the allegations in paragraphs
21 1 through 32 above.

22 34. Upon information and belief Plaintiff alleges that Defendants have
23 violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"), specifically
24 section 1030(a)(2)(A) of the CFAA, by intentionally accessing a computer without
25 authorization or exceeding authorized access, and thereby obtaining information
26 contained in financial records of one or more financial institutions or of one or more
27 card issuers as defined in section 1602(n) of title 15, or contained in one or more files
28 of a consumer reporting agency on a consumer, as such terms are defined in the Fair

1 Credit Reporting Act (15 U.S.C. 1681, *et seq.*).

2 35. Upon information and belief, Plaintiff further alleges that Defendants have
3 violated the CFAA, specifically section 1030(a)(2)(C) of the CFAA, by intentionally
4 accessing a computer without authorization or exceeding authorized access, and
5 thereby obtaining information from any protected computer which, pursuant to the
6 CFAA, is a computer used in or affecting interstate commerce or communication.

7 36. Upon information and belief, Plaintiff further alleges that Defendants have
8 violated the CFAA, specifically section 1030(a)(4) of the CFAA, by knowingly and
9 with intent to defraud, accessing a protected computer without authorization or
10 exceeding authorized access, and by means of such conduct furthering the intended
11 fraud and obtaining one or more things of value.

12 37. Plaintiff has suffered damages or losses as a result of Defendants'
13 violations of the CFAA far in excess of \$5,000. These damages and losses to Plaintiff
14 include but are not limited to direct costs, incurred during any one-year period, of
15 investigating and responding to Defendants' violations of the CFAA in excess of
16 \$5,000 in value.

17 **SECOND CLAIM FOR RELIEF**

18 **(Violation of the California Computer Data Access and Fraud Act)**

19 **(Cal. Penal Code § 520)**

20 **(Against all Defendants)**

21 38. Plaintiff incorporates herein by this reference the allegations in paragraphs
22 1 through 32 above.

23 39. Plaintiff owns data that is stored on a copy of a hard drive or other
24 device(s) that Defendants own and operate and claim to have obtained of Plaintiff's
25 computer and that Defendants claim to have obtained by hacking into Plaintiff's
26 encrypted iPhone backup.

27 40. Defendants have violated California Penal Code § 502(c)(1) by knowingly
28 accessing and without permission taking and using data from Plaintiff's devices or

1 “cloud” storage, including but not limited to, Plaintiff’s encrypted iPhone backup to
2 devise or execute a scheme to defraud or deceive, or to wrongfully obtain money,
3 property, or data.

4 41. Defendants also have violated California Penal Code § 502(c)(2) by
5 knowingly and without permission accessing, taking, copying, and making use of
6 programs, data, and files from Plaintiff’s devices or “cloud” storage, including but not
7 limited to, Plaintiff’s encrypted iPhone backup.

8 42. Defendants also have violated California Penal Code § 502(c)(3) by
9 knowingly and without permission using or causing to be used computer services as
10 that term is defined in the statute.

11 43. Defendants also have violated California Penal Code § 502(c)(7) by
12 knowingly and without permission accessing, or causing to be accessed, data and files
13 from Plaintiff’s devices or “cloud” storage, including but not limited to, Plaintiff’s
14 encrypted iPhone backup.

15 44. As a direct and proximate result of Defendants’ unlawful conduct within
16 the meaning of California Penal Code § 502, Defendants have caused damage to
17 Plaintiff in an amount to be proven at trial.

18 45. The aforementioned acts of Defendants were willful and malicious in that
19 they were done with the deliberate intent to injure Plaintiff. Plaintiff is therefore
20 entitled to punitive damages in an amount to be proven at trial.

21 46. Plaintiff has also suffered irreparable injury from these acts, and due to the
22 continuing threat of such injury, has no adequate remedy at law, entitling Plaintiff to
23 injunctive and other equitable relief.

24 47. Plaintiff is also entitled to recover his reasonable attorneys’ fees pursuant
25 to California Penal Code § 502(e).

THIRD CLAIM FOR RELIEF

(Cal. Bus. & Prof. Code §§ 17200 *et seq.*)

(Against All Defendants)

1
2
3
4 48. Plaintiff incorporates herein by this reference the allegations in paragraphs
5 1 through 32 above.

6 49. California Business & Professions Code sections 17200 *et seq.* state that
7 no business may engage in unfair competition. According to section 17200, “unfair
8 shall mean and include any unlawful, unfair or fraudulent business act or practice and
9 unfair, deceptive, untrue or misleading advertising.”

10 50. By engaging in the conduct alleged herein, Defendants have engaged in
11 unfair and unlawful activities in violation of the CFAA and California Penal Code
12 section 502

13 51. Plaintiff is informed and believes and thereon alleges that the Defendants
14 will continue to do these acts unless the Court orders Defendants to cease and desist,
15 and, therefore, Plaintiff requests injunctive relief pursuant to California Business and
16 Professions Code section 17203.

17 52. Based on the above allegations, including the alleged violations of the
18 CFAA and California Penal Code section 502, Plaintiff is entitled to injunctive and
19 equitable relief to stop Defendants from continuing to engage in their unlawful and
20 unfair conduct with respect to Plaintiff and as necessary to restore to Plaintiff any
21 money or property which Defendants have acquired by means of such unlawful and
22 unfair conduct; restitution in an amount to be determined at trial; attorneys’ fees and
23 costs as may be permitted by law; and any other relief as may be proper.

24 **JURY TRIAL DEMAND**

25 Plaintiff hereby respectfully demands a jury trial in this action for all causes of
26 action for which a jury trial is available.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief as follows:

- A. For general damages to be proven at trial;
- B. For punitive damages to be proven at trial for Defendants’ willful and deliberate actions including their unauthorized access, tampering with, manipulation and copying of, and damage to Plaintiff’s data;
- C. For disgorgement of all money obtained by Defendants as a result of their unlawful and otherwise wrongful conduct;
- D. For prejudgment interest;
- E. For an order awarding Plaintiff his reasonable attorneys’ fees and costs;
- F. For a preliminary and permanent injunction restraining Defendants, their officers, agents, employees, and attorneys, and those in active concert or participation with any of them, from:


(1) Accessing, tampering with, manipulating or copying Plaintiff’s data;
and

(2) Restoring to Plaintiff any money or property which Defendants have acquired by means of such unlawful and unfair conduct including but not limited to any data in their possession that was sent to them or that they obtained from any account, device/hard drive, back up files, “cloud” files or copies of the same belonging to Plaintiff;

G. For such other and further relief as this Court may deem to be just and proper.


Dated: September 13, 2023

Respectfully submitted,
WINSTON & STRAWN LLP

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

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

EARLY SULLIVAN WRIGHT
GIZER & McRAE LLP

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