

**BEFORE THE ATTORNEY DISCIPLINE
PROBABLE CAUSE COMMITTEE
OF THE SUPREME COURT OF ARIZONA**

**IN THE MATTER OF A NON-MEMBER
OF THE STATE BAR OF ARIZONA,**

No. 23-0051

PROBABLE CAUSE ORDER

KURT OLSEN

Respondent.

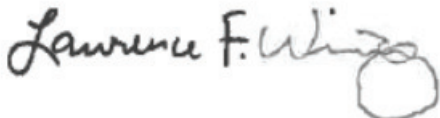
The Attorney Discipline Probable Cause Committee of the Supreme Court of Arizona (“Committee”) reviewed this matter on December 8, 2023, pursuant to Rules 50 and 55, Ariz. R. Sup. Ct., for consideration of the State Bar’s Report of Investigation and Recommendation and Respondent's Response.

By a vote of 7-0-2¹, the Committee finds probable cause exists to file a complaint against Respondent in File No. 23-0051.

IT IS THEREFORE ORDERED pursuant to Rule 55(c) and 58(a), Ariz. R. Sup. Ct., authorizing the State Bar counsel to prepare and file a complaint with the Disciplinary Clerk.

Parties may not file motions for reconsideration of this Order.

DATED this ___11___ day of December, 2023.



Judge (ret.) Lawrence F. Winthrop,
Chair, Attorney Discipline Probable Cause Committee of the Supreme Court

¹ Committee member Judge Cynthia Bailey and Brent Vermeer did not participate in this matter.

Original filed this 11th day
of December, 2023, with:

Lawyer Regulation Records Manager
State Bar of Arizona
4201 N. 24th St., Suite 100
Phoenix, Arizona 85016-6266

Copy emailed this 11th day
of December, 2023, to:

Kurt Olsen
1250 Connecticut Ave., NW, Suite 700
Washington, DC 20036
Email: ko@olsenlawpc.com
Respondent

Copy emailed this 11th day
of December, 2023, to:

Attorney Discipline Probable Cause Committee
Of the Supreme Court of Arizona
1501 West Washington Street, Suite 104
Phoenix, Arizona 85007
E-mail: ProbableCauseComm@courts.az.gov

Lawyer Regulation Records Manager
State Bar of Arizona
4201 N. 24th St., Suite 100
Phoenix, Arizona 85016-6266
E-mail: LRO@staff.azbar.org

By: /s/Melissa Quintana
HFP/KAG/mq



Assistant's Direct Line: (602) 340-7386

Sent via email only: ko@olsenlawpc.com

December 11, 2023

PERSONAL AND CONFIDENTIAL

Kurt Olsen
1250 Connecticut Ave., NW, Suite 700
Washington, DC 20036

Re: File No: 23-0051
Complainant: State Bar of Arizona

Dear Mr. Olsen:

The Attorney Discipline Probable Cause Committee of the Supreme Court of Arizona has entered, in the above-referenced matter, the enclosed Probable Cause Order.

Before a formal complaint is filed and litigation commenced, this matter may be resolved by an agreement for discipline by consent. Rule 57, Ariz. R. Sup. Ct., allows a Respondent to tender conditional admissions to a charge in exchange for a stated form of discipline. An agreement for discipline by consent saves time and costs and provides an opportunity for you to participate in developing a formal statement of the case for the record.

To prevent unnecessary delay, I plan on continuing to prepare our file for adjudication. In the meantime, if you wish to speak to me about possible settlement, or wish to discuss the case further, please feel free to contact me at (602) 340-7386. I welcome the opportunity to further discuss this matter with you.

I understand that you are, at this point, unrepresented. This letter is not intended to provide legal advice. If you have any questions about the process, I urge you to seek counsel.

Thank you again for your assistance in this matter and I look forward to speaking with you in the near future.

Sincerely,

/s/Hunter F. Perlmeter

Hunter F. Perlmeter
Bar Counsel

HFP/mq

Enclosure

/s/Kelly A. Goldstein

Kelly A. Goldstein
Bar Counsel

Sandra Montoya

From: Melissa Quintana
Sent: Monday, December 11, 2023 4:03 PM
To: 'ko@olsenlawpc.com'
Subject: State Bar File No. 23-0051 - Olsen
Attachments: Letter to R Transmitting ADPCC Order.pdf; 23-0051 Olsen - Order of Probable Cause.pdf

Dear Mr. Olsen,

Attached is a letter from Bar Counsel Hunter F. Perlmeter and Kelly A. Goldstein, regarding the above-referenced matter. Also attached is a copy of the Probable Cause Order.

Thank you,



Melissa Quintana, Legal Secretary

State Bar of Arizona

4201 N. 24th St., Suite 100 | Phoenix, AZ 85016-6266

T : 602.340.7386 **F :** 602.416.7586

EMAIL: Melissa.Quintana@staff.azbar.org

www.azbar.org

Serving the public and enhancing the legal profession.

This electronic mail message contains CONFIDENTIAL information which is (a) ATTORNEY - CLIENT PRIVILEGED COMMUNICATION, WORK PRODUCT, PROPRIETARY IN NATURE, OR OTHERWISE PROTECTED BY LAW FROM DISCLOSURE, and (b) intended only for the use of the Addressee(s) named herein. If you are not an Addressee, or the person responsible for delivering this to an Addressee, you are hereby notified that reading, copying, or distributing this message is prohibited. If you have received this electronic mail message in error, please reply to the sender and take the steps necessary to delete the message completely from your computer system.

Sandra Montoya

From: Kurt Olsen <ko@olsenlawpc.com>
Sent: Monday, November 6, 2023 1:50 PM
To: Hunter F. Perlmeter
Cc: Kelly Goldstein; Melissa Quintana
Subject: Re: ADPCC Response re: File Nos. 23-0051 and 23-1164

Thank you.

From: "Hunter F. Perlmeter" <hunter.perlmeter@staff.azbar.org>
Date: Monday, November 6, 2023 at 3:49 PM
To: Kurt Olsen <ko@olsenlawpc.com>
Cc: Kelly Goldstein <Kelly.Goldstein@staff.azbar.org>, Melissa Quintana <Melissa.Quintana@staff.azbar.org>
Subject: RE: ADPCC Response re: File Nos. 23-0051 and 23-1164

Received, Kurt. Thanks.

Best,
Hunter



Hunter Perlmeter, Senior Bar Counsel

State Bar of Arizona

4201 N. 24th St., Suite 100 | Phoenix, AZ 85016-6266

T : 602.340.7274 **F :** 602.416.7474

EMAIL: hunter.perlmeter@staff.azbar.org

www.azbar.org

Serving the public and enhancing the legal profession.

From: Kurt Olsen <ko@olsenlawpc.com>
Sent: Monday, November 6, 2023 1:45 PM
To: Hunter F. Perlmeter <hunter.perlmeter@staff.azbar.org>
Cc: Kelly Goldstein <Kelly.Goldstein@staff.azbar.org>
Subject: ADPCC Response re: File Nos. 23-0051 and 23-1164

Dear Hunter,

Attached is my response to the ADPCC re: the Report of Investigation in the above-referenced matters. As discussed, please forward this to the ADPCC. Also, please acknowledge receipt of this email. Thank you.

Sincerely,

Kurt

Kurt B. Olsen

OLSEN LAW, P.C.

1250 Connecticut Ave., NW, Ste. 700

Washington DC 20036

(202) 408-7025

ko@olsenlawpc.com

The information in this transmittal may be legally privileged, confidential, and/or otherwise protected by law from disclosure, and is intended only for the recipient(s) listed above. If you are neither the intended recipient(s) nor a person responsible for the delivery of this transmittal to the intended recipient(s), you are hereby notified that any distribution or copying of this transmittal is prohibited. If you have received this transmittal in error, please notify Olsen Law P.C. immediately by return e-mail and take the steps necessary to delete it completely from your computer system. Thank

you. **Beware External Email - Think Before You Act**

Links and attachments should not be opened unless expected or verified

The information in this transmittal may be legally privileged, confidential, and/or otherwise protected by law from disclosure, and is intended only for the recipient(s) listed above. If you are neither the intended recipient(s) nor a person responsible for the delivery of this transmittal to the intended recipient(s), you are hereby notified that any distribution or copying of this transmittal is prohibited. If you have received this transmittal in error, please notify Olsen Law P.C. immediately by return e-mail and take the steps necessary to delete it completely from your computer system. Thank

you. **Beware External Email - Think Before You Act**

Links and attachments should not be opened unless expected or verified

Sandra Montoya

From: Hunter F. Perlmeter
Sent: Friday, November 3, 2023 2:17 PM
To: Kurt Olsen; Melissa Quintana
Cc: Kelly Goldstein
Subject: RE: State Bar File Nos. 23-0051 & 23-1164 - Olsen

Our office just forwards to ADPCC whatever we receive from a Respondent. What you choose to submit is entirely up to you. If you have any other questions regarding the process, it's set forth in Rule 55 Ariz. R. Sup. Ct.



Hunter Perlmeter, Senior Bar Counsel
State Bar of Arizona

4201 N. 24th St., Suite 100 | Phoenix, AZ 85016-6266
T : 602.340.7274 **F** : 602.416.7474
EMAIL: hunter.perlmeter@staff.azbar.org
www.azbar.org

Serving the public and enhancing the legal profession.

From: Kurt Olsen <ko@olsenlawpc.com>
Sent: Friday, November 3, 2023 2:02 PM
To: Hunter F. Perlmeter <hunter.perlmeter@staff.azbar.org>; Melissa Quintana <Melissa.Quintana@staff.azbar.org>
Cc: Kelly Goldstein <Kelly.Goldstein@staff.azbar.org>
Subject: Re: State Bar File Nos. 23-0051 & 23-1164 - Olsen

Thank you, Hunter. I assume I can attach exhibits to my response, including my prior responses, is that correct?

Kurt

From: "Hunter F. Perlmeter" <hunter.perlmeter@staff.azbar.org>
Date: Friday, November 3, 2023 at 4:46 PM
To: Kurt Olsen <ko@olsenlawpc.com>, Melissa Quintana <Melissa.Quintana@staff.azbar.org>
Cc: Kelly Goldstein <Kelly.Goldstein@staff.azbar.org>
Subject: RE: State Bar File Nos. 23-0051 & 23-1164 - Olsen

Hi, Kurt:

ADPCC will not have access to what you've previously submitted to the State Bar.

Best,
Hunter



Hunter Perlmeter, Senior Bar Counsel
State Bar of Arizona

4201 N. 24th St., Suite 100 | Phoenix, AZ 85016-6266

T : 602.340.7274 F : 602.416.7474

EMAIL: hunter.perlmeter@staff.azbar.org

www.azbar.org

Serving the public and enhancing the legal profession.

From: Kurt Olsen <ko@olsenlawpc.com>

Sent: Friday, November 3, 2023 1:42 PM

To: Melissa Quintana <Melissa.Quintana@staff.azbar.org>

Cc: Hunter F. Perlmeter <hunter.perlmeter@staff.azbar.org>; Kelly Goldstein <Kelly.Goldstein@staff.azbar.org>

Subject: Re: State Bar File Nos. 23-0051 & 23-1164 - Olsen

Dear Ms. Quintana,

With respect to any response from me to these charges, are my original responses part of the record or do they need to be resubmitted? Thank you.

Kurt Olsen

From: Melissa Quintana <Melissa.Quintana@staff.azbar.org>

Date: Wednesday, October 18, 2023 at 6:00 PM

To: Kurt Olsen <ko@olsenlawpc.com>

Subject: State Bar File Nos. 23-0051 & 23-1164 - Olsen

Dear Mr. Olsen,

Attached please find a Letter to you from Bar Counsel Kelly A. Goldstein and Hunter F. Perlmeter.

Thank you,



Melissa Quintana, Legal Secretary

State Bar of Arizona

4201 N. 24th St., Suite 100 | Phoenix, AZ 85016-6266

T : 602.340.7386 F : 602.416.7586

EMAIL: Melissa.Quintana@staff.azbar.org

www.azbar.org

Serving the public and enhancing the legal profession.

This electronic mail message contains CONFIDENTIAL information which is (a) ATTORNEY - CLIENT PRIVILEGED COMMUNICATION, WORK PRODUCT, PROPRIETARY IN NATURE, OR OTHERWISE PROTECTED BY LAW FROM DISCLOSURE, and (b) intended only for the use of the Addressee(s) named herein. If you are not an Addressee, or the

person responsible for delivering this to an Addressee, you are hereby notified that reading, copying, or distributing this message is prohibited. If you have received this electronic mail message in error, please reply to the sender and take the steps necessary to delete the message completely from your computer system.

The information in this transmittal may be legally privileged, confidential, and/or otherwise protected by law from disclosure, and is intended only for the recipient(s) listed above. If you are neither the intended recipient(s) nor a person responsible for the delivery of this transmittal to the intended recipient(s), you are hereby notified that any distribution or copying of this transmittal is prohibited. If you have received this transmittal in error, please notify Olsen Law P.C. immediately by return e-mail and take the steps necessary to delete it completely from your computer system. Thank you. **Beware External Email - Think Before You Act**

Links and attachments should not be opened unless expected or verified

The information in this transmittal may be legally privileged, confidential, and/or otherwise protected by law from disclosure, and is intended only for the recipient(s) listed above. If you are neither the intended recipient(s) nor a person responsible for the delivery of this transmittal to the intended recipient(s), you are hereby notified that any distribution or copying of this transmittal is prohibited. If you have received this transmittal in error, please notify Olsen Law P.C. immediately by return e-mail and take the steps necessary to delete it completely from your computer system. Thank you. **Beware External Email - Think Before You Act**

Links and attachments should not be opened unless expected or verified

Sandra Montoya

From: Melissa Quintana
Sent: Wednesday, October 18, 2023 3:00 PM
To: 'ko@olsenlawpc.com'
Subject: State Bar File Nos. 23-0051 & 23-1164 - Olsen
Attachments: Letter to R Transmitting ROI.pdf

Dear Mr. Olsen,

Attached please find a Letter to you from Bar Counsel Kelly A. Goldstein and Hunter F. Perlmeter.

Thank you,



Melissa Quintana, Legal Secretary

State Bar of Arizona

4201 N. 24th St., Suite 100 | Phoenix, AZ 85016-6266

T : 602.340.7386 F : 602.416.7586

EMAIL: Melissa.Quintana@staff.azbar.org

www.azbar.org

Serving the public and enhancing the legal profession.

This electronic mail message contains CONFIDENTIAL information which is (a) ATTORNEY - CLIENT PRIVILEGED COMMUNICATION, WORK PRODUCT, PROPRIETARY IN NATURE, OR OTHERWISE PROTECTED BY LAW FROM DISCLOSURE, and (b) intended only for the use of the Addressee(s) named herein. If you are not an Addressee, or the person responsible for delivering this to an Addressee, you are hereby notified that reading, copying, or distributing this message is prohibited. If you have received this electronic mail message in error, please reply to the sender and take the steps necessary to delete the message completely from your computer system.



Assistant's Direct Line: (602) 340-7386

Sent via email only: ko@olsenlawpc.com

October 18, 2023

PERSONAL AND CONFIDENTIAL

Kurt Olsen
1250 Connecticut Ave. NW, Suite 700
Washington, DC 20036

Re: File Nos: 23-0051 and 23-1164
Complainant: State Bar of Arizona

Dear Mr. Olsen:

We have completed our investigation into the matters listed above. Attached is the investigative report that we intend to submit to the Attorney Discipline Probable Cause Committee ("ADPCC"). As you can see, we recommend an Order of Probable Cause. ADPCC will consider this report at its next available agenda.

You have until **November 6, 2023 at 3:00 p.m.**, if you wish to submit a written summary of your response to the charge to persuade the ADPCC the recommended disposition is not warranted or to record your agreement with the recommended disposition. We will send such a submittal to ADPCC with the report of investigation. If you wish to submit such a statement, please mail or deliver it to my attention, but addressed to Members of the Attorney Discipline Probable Cause Committee. A letter format is satisfactory, and I must receive it by the date listed above. We may not extend this time period unless you establish substantial good cause, in writing to me. Thank you for your cooperation.

If the ADPCC imposes a sanction, you will also be charged costs pursuant to Rule 60(d), Ariz. R. Sup. Ct. The Supreme Court of Arizona's schedule of costs is online at <https://www.azbar.org/media/fy2ahbcl/fee-schedule.pdf>.

Sincerely,

/s/Kelly A. Goldstein

Kelly A. Goldstein
Bar Counsel

/s/Hunter F. Perlmeter

Hunter F. Perlmeter
Bar Counsel

KAG/mq

Enclosure

Sandra Montoya

From: Jennifer Smith
Sent: Wednesday, February 22, 2023 11:36 AM
To: Kurt Olsen
Subject: 23-0051 - Olsen; Arizona : Non-Public
Attachments: Letter to R Response Received Letterhead.pdf

Please find the attached.

Thank you,

The attached is being sent by email only. If you have any questions, please email the assigned Bar Counsel at: kelly.flood@staff.azbar.org.



Jennifer Smith, Legal Secretary

State Bar of Arizona

4201 N. 24th St., Suite 100 | Phoenix, AZ 85016-6266

T : 602.340.7272 **F** : 602.416.7472

EMAIL: jennifer.smith@staff.azbar.org

www.azbar.org

Serving the public and enhancing the legal profession.

This electronic mail message contains CONFIDENTIAL information which is (a) ATTORNEY - CLIENT PRIVILEGED COMMUNICATION, WORK PRODUCT, PROPRIETARY IN NATURE, OR OTHERWISE PROTECTED BY LAW FROM DISCLOSURE, and (b) intended only for the use of the Addressee(s) named herein. If you are not an Addressee, or the person responsible for delivering this to an Addressee, you are hereby notified that reading, copying, or distributing this message is prohibited. If you have received this electronic mail message in error, please reply to the sender and take the steps necessary to delete the message completely from your computer system.



Assistant's Direct Line: (602)340-7272

February 22, 2023

PERSONAL AND CONFIDENTIAL

Kurt Olsen
1250 Connecticut Ave., NW, Suite 700
Washington, DC 20036
Via email, only, to: ko@olsenlawpc.com

Re: File No: 23-0051
Complainant: State Bar of Arizona

Dear Mr. Olsen:

This acknowledges receipt of your correspondence dated February 21, 2023, in which you respond to the charges. In most cases, an investigator will be contacting you shortly for more information or to schedule an interview.

After our investigation is completed, this matter may be dismissed by bar counsel or a recommendation for discipline or diversion made to the Attorney Discipline Probable Cause Committee. You will be advised of the recommendation and provided an opportunity for input.

Sincerely,

/s/Hunter F. Perlmeter

/s/Kelly A. Goldstein

Hunter F. Perlmeter and
Kelly A. Goldstein
Bar Counsel

HFP/jas

Enclosure

Sandra Montoya

From: Kurt Olsen <ko@olsenlawpc.com>
Sent: Tuesday, February 21, 2023 4:28 PM
To: Jennifer Smith; Hunter F. Perlmeter; Kelly Goldstein
Subject: Re: State Bar File No. 23-0051 - Olsen
Attachments: 022123 AZ Bar response.pdf

Dear Hunter and Kelly,

Please see my attached response to the above-referenced matter.

All the best,

Kurt

From: Jennifer Smith <Jennifer.Smith@staff.azbar.org>
Date: Friday, January 13, 2023 at 11:03 AM
To: "Hunter F. Perlmeter" <hunter.perlmeter@staff.azbar.org>, Kurt Olsen <ko@olsenlawpc.com>, Kelly Goldstein <Kelly.Goldstein@staff.azbar.org>
Subject: RE: State Bar File No. 23-0051 - Olsen

New date to submit your response will be February 21.

Thank you.

From: Hunter F. Perlmeter <hunter.perlmeter@staff.azbar.org>
Sent: Thursday, January 12, 2023 4:01 PM
To: Kurt Olsen <ko@olsenlawpc.com>; Kelly Goldstein <Kelly.Goldstein@staff.azbar.org>; Jennifer Smith <Jennifer.Smith@staff.azbar.org>
Subject: Re: State Bar File No. 23-0051 - Olsen

Hi, Kurt. No problem. Jennifer will send you a new response date.

Best,
Hunter

Get [Outlook for iOS](#)

From: Kurt Olsen <ko@olsenlawpc.com>
Sent: Thursday, January 12, 2023 3:59:08 PM
To: Hunter F. Perlmeter <hunter.perlmeter@staff.azbar.org>; Kelly Goldstein <Kelly.Goldstein@staff.azbar.org>
Subject: Re: State Bar File No. 23-0051 - Olsen

Dear Hunter and Kelly,

I understand that a 20-day courtesy extension to file a written response to this matter is permissible under Arizona R. Sup. Ct. Rule 55(b)1.A. I'd like to request such an extension. Please let me know. Thank you.

Sincerely,

Kurt Olsen

From: Jackie Brokaw <Jackie.Brokaw@staff.azbar.org>

Date: Tuesday, January 10, 2023 at 3:00 PM

To: Kurt Olsen <ko@olsenlawpc.com>

Subject: State Bar File No. 23-0051 - Olsen

Good afternoon,

Attached is a letter to you from Bar Counsel Hunter Perlmeter and Kelly Goldstein. There are two enclosures to the letter.

Thank you,

Jackie



Jackie Brokaw, Lead Legal Secretary

State Bar of Arizona

4201 N. 24th St., Suite 100 | Phoenix, AZ 85016-6266

T : 602.340.7250 **F :** 602.416.7450

EMAIL: Jackie.Brokaw@staff.azbar.org

www.azbar.org

Serving the public and enhancing the legal profession.

This electronic mail message contains CONFIDENTIAL information which is (a) ATTORNEY - CLIENT PRIVILEGED COMMUNICATION, WORK PRODUCT, PROPRIETARY IN NATURE, OR OTHERWISE PROTECTED BY LAW FROM DISCLOSURE, and (b) intended only for the use of the Addressee(s) named herein. If you are not an Addressee, or the person responsible for delivering this to an Addressee, you are hereby notified that reading, copying, or distributing this message is prohibited. If you have received this electronic mail message in error, please reply to the sender and take the steps necessary to delete the message completely from your computer system.

The information in this transmittal may be legally privileged, confidential, and/or otherwise protected by law from disclosure, and is intended only for the recipient(s) listed above. If you are neither the intended recipient(s) nor a person responsible for the delivery of this transmittal to the intended recipient(s), you are hereby notified that any distribution or copying of this transmittal is prohibited. If you have received this transmittal in error, please notify Olsen Law P.C. immediately by return e-mail and take the steps necessary to delete it completely from your computer system. Thank you. **Beware External Email - Think Before You Act**

Links and attachments should not be opened unless expected or verified

The information in this transmittal may be legally privileged, confidential, and/or otherwise protected by law from disclosure, and is intended only for the recipient(s) listed above. If you are neither the intended recipient(s) nor a person responsible for the delivery of this transmittal to the intended recipient(s), you are hereby notified that any distribution or copying of this transmittal is prohibited. If you have received this transmittal in error, please notify Olsen Law P.C. immediately by return e-mail and take the steps necessary to delete it completely from your computer system. Thank

you. **Beware External Email - Think Before You Act**
Links and attachments should not be opened unless expected or verified

OLSEN LAW, P.C.

KURT B. OLSEN

ATTORNEY AT LAW
1250 CONNECTICUT AVENUE, N.W., SUITE 700, WASHINGTON, DC 20036
(202) 408-7025
KO@OLSENLAWPC.COM

February 21, 2023

VIA EMAIL

Hunter F. Perlmeter
Kelly A. Goldstein
State Bar of Arizona
4201 N. 24th Street, Suite 100
Phoenix, AZ 85016-6266

Re: State Bar File No. 23-0051 - Olsen

Dear Mr. Perlmeter and Ms. Goldstein,

This letter serves as my response to the above-referenced matter. I have been a member of the Maryland Bar for over 30 years and a member of the District of Columbia Bar for over 28 years. I have never received a complaint by any client or any opposing party, much less been sanctioned, in these many years of practice. I started out practicing law at one of the finest law firms in the Country, Kirkland & Ellis, P.C., and during my career I have represented hundreds of businesses and individuals from all walks of life. Before becoming an attorney, I graduated from the U.S. Naval Academy, and served our Country as a U.S. Navy SEAL. Ethics, honor, and integrity are ingrained in my soul.

With respect to the substantive bar charge against me, I hereby incorporate by reference the response of my co-counsel, Andrew Parker, in File No. 22-2766. The bar complaints against me and Mr. Parker are based on the same court case and facts. Mr. Parker also sought a protective order for his response in light of the pending appeal to the Ninth Circuit of the district court's order dismissing the action, also at issue in these bar complaints. Disclosure of the contents of Mr. Parker's response would be prejudicial to us in that appeal because it would provide appellees access to our client confidential information, attorney work product and mental impressions of counsel which are necessarily included in the response to this bar charge.

For the reasons discussed above and in Mr. Parker's response, this investigation should be terminated, and the matter dismissed. If you have any questions or need further information, please do not hesitate to contact me.

Sincerely,



Kurt B. Olsen, Esq.

Sandra Montoya

From: Jackie Brokaw
Sent: Tuesday, January 10, 2023 1:00 PM
To: ko@olsenlawpc.com
Subject: State Bar File No. 23-0051 - Olsen
Attachments: Letter to R Initial Screen letterhead.pdf; Initial Charge Amended Complaint.pdf; Initial Charge.pdf

Good afternoon,

Attached is a letter to you from Bar Counsel Hunter Perlmeter and Kelly Goldstein. There are two enclosures to the letter.

Thank you,

Jackie



Jackie Brokaw, Lead Legal Secretary

State Bar of Arizona

4201 N. 24th St., Suite 100 | Phoenix, AZ 85016-6266

T : 602.340.7250 **F :** 602.416.7450

EMAIL: Jackie.Brokaw@staff.azbar.org

www.azbar.org

Serving the public and enhancing the legal profession.

This electronic mail message contains CONFIDENTIAL information which is (a) ATTORNEY - CLIENT PRIVILEGED COMMUNICATION, WORK PRODUCT, PROPRIETARY IN NATURE, OR OTHERWISE PROTECTED BY LAW FROM DISCLOSURE, and (b) intended only for the use of the Addressee(s) named herein. If you are not an Addressee, or the person responsible for delivering this to an Addressee, you are hereby notified that reading, copying, or distributing this message is prohibited. If you have received this electronic mail message in error, please reply to the sender and take the steps necessary to delete the message completely from your computer system.



Assistant's Direct Line: (602) 340-7272

January 10, 2023

PERSONAL AND CONFIDENTIAL

Kurt Olsen
1250 Connecticut Ave., NW, Suite 700
Washington, DC 20036
Via email, only, to: ko@olsenlawpc.com

Re: File No: 23-0051
Complainant: State Bar of Arizona

Dear Mr. Olsen:

The State Bar has received information concerning your professional conduct that warrants a screening investigation pursuant to Rule 55(b), Ariz. R. Sup. Ct. At this point, the matter is not considered a formal complaint, but rather a "bar charge" that is being investigated through a "screening investigation." Your participation in the screening investigation is extremely important, as Bar Counsel will make a recommendation at the end of the investigation as to the disposition of this matter. Pursuant to ER 8.1(b) and Rule 54(d), Ariz. R. Sup. Ct., you have a duty to cooperate with this investigation. Failure to fully and honestly respond to, or cooperate with, the investigation is, in itself, grounds for discipline.

A copy of the information received by the State Bar has been included with this letter. Please assure that a written response to the enclosed information is in the State Bar's office, directed to my attention, by:

5:00 pm, February 1, 2023

In addition to your written response, an investigator from our office or I may contact you to discuss this matter. Do not send your written response or a copy of your response directly to the Complainant. If you cannot file a timely response, you should contact my office immediately. Please also include the above-referenced file number on all correspondence concerning this matter. You must submit **an original and one copy** of your written response. If you do not submit a copy with your response, you will be charged \$.25 per page for copying your response.

The ethical rules that should be addressed in your response include, but are not limited to: ER 1.1, ER 1.3, ER 3.1, ER 3.2, ER 3.3, ER 3.4(c), ER 4.4, ER 8.4(c), and ER 8.4(d).

While the following is not an exhaustive list of the issues the State Bar may investigate, please ensure that your response addresses the following:

- a. Whether you alleged or implied that Arizona does not use paper ballots (e.g., FAC ¶¶ 58, 71, 153, 168, 171; Mot. for Prelim. Inj. at 2);

- b. Your reliance upon *Curling v. Raffensperger* notwithstanding that the issues referenced with respect to Georgia voting do not exist in Arizona (e.g., FAC ¶¶ 4, 81-85, 139, 146; Mot. for PI at 9-10; Opp'n to Ariz. Sec. of State Mot. to Dismiss at 1, 11, 13), and the argument that the "voting system at issue in Georgia is used in ... Arizona," FAC ¶ 146; see also FAC ¶ 139;
- c. Your argument that Arizona uses "electronic voting machines" (e.g., FAC ¶¶ 6, 17, 24-31, 90, 125, 144, 152) when only a small portion of the population can cast a vote using a computer and paper ballots are generated;
- d. Your decision to wait until seven weeks after filing the Complaint to move for a preliminary injunction, five months before the general election;
- e. Your argument that Arizona voting systems are connected to the internet and decision not to disclose the special master's report to the contrary;
- f. Concerning standing: whether you alleged that the threatened injury was "certainly impending" as required under *Clapper v. Amnesty Int'l USA*;
- g. Whether Alan Dershowitz authorized you to add his electronic signature to pleadings (see Application for OSC); and
- h. Whether you made any changes to your allegations and strategy after receiving the May 20, 2022 letter from Emily Craiger and, if not, why no such changes were made.

A copy of your response will be sent to the Complainant and may become public record upon disposition of the matter. You may make a request that certain information in your response remain confidential pursuant to Rule 70(g) Ariz. R. Sup. Ct. **Any such request must be made in a letter separate from your response** and must set forth the reason for the request. We will forward your request to the Presiding Disciplinary Judge who will rule on it. You must specify whether you want to keep the information from the public, but not the complainant, or from both the public and the complainant. At the time you make such a request, you must submit the information for which confidentiality is requested as part of your request. You should also submit a redacted copy to remain in the public portion of the file, as the rules require some type of response to remain in the public portion of the file. Requests for confidentiality are only granted sparingly and only upon good cause shown. If your request for confidentiality is denied, the information or documents in question will not be returned to you, but will become public upon disposition of the matter.

The State Bar has a diversion program which, in some cases, may provide an alternative to traditional discipline. Diversion is a confidential rehabilitative program available to lawyers whose ethical misconduct is of a non-serious nature and who may benefit from one or more of the State Bar's remedial programs, such as the Member Assistance Program (MAP) or the Law Office Management Assistance Program (LOMAP). Diversion is not available in cases of serious misconduct or for conduct involving dishonesty, self-dealing, or breach of a fiduciary duty. Participation in diversion is voluntary. If you would like more information about the State Bar's diversion program, you may review the Diversion Guidelines on-line at:

<http://www.azcourts.gov/Portals/22/admorder/Orders10/2010-127.pdf>

If, after reviewing the guidelines, you believe your case may qualify for diversion, please submit a written request with a statement of why you believe diversion is appropriate along with your response.

Thank you for your anticipated cooperation.

Sincerely,

/s/Hunter F. Perlmeter

/s/Kelly A. Goldstein

Hunter F. Perlmeter and
Kelly A. Goldstein
Bar Counsel

HFP/jlb

Enclosure

1 **WO**

2
3
4
5
6 **IN THE UNITED STATES DISTRICT COURT**
7 **FOR THE DISTRICT OF ARIZONA**
8

9 Kari Lake, *et al.*,
10 Plaintiffs,

11 v.

12 Katie Hobbs, *et al.*,
13 Defendants.
14

No. CV-22-00677-PHX-JJT

ORDER

15 At issue is the Federal Rule of Civil Procedure 11 and 28 U.S.C. § 1927 Motion for
16 Sanctions (Doc. 97, “Mot.”) filed by Defendants Bill Gates, Clint Hickman, Jack Sellers,
17 Thomas Galvin, and Steve Gallardo in their official capacities as members of the Maricopa
18 County Board of Supervisors (hereinafter referred to collectively as “Maricopa County
19 Defendants”), to which Plaintiffs Kari Lake and Mark Finchem filed a Response (Doc. 99,
20 “Resp.”), and the Maricopa County Defendants filed a Reply (Doc. 102, “Reply”). The
21 Court finds this matter appropriate for disposition without oral argument. LRCiv 7.2(f).
22 For the reasons set forth below, the Court grants the Maricopa County Defendants’ motion.

23 **I. BACKGROUND**

24 In this case, Plaintiffs challenged the procedures for administering elections in
25 Arizona and sought an injunction compelling Defendants—election officials at the state
26 and county levels—to follow alternative procedures for collecting, storing, counting, and
27 tabulating votes in the 2022 midterm election. (Doc. 3, Plaintiffs’ first Amended Complaint
28 (“FAC”) ¶¶ 1, 153.) These alternative procedures included requiring voters to cast their

1 votes on paper ballots and ordering election administrators to count every ballot cast by
2 hand. (*Id.* ¶ 153.) On August 26, 2022, the Court granted motions to dismiss filed by
3 Defendants and dismissed Plaintiffs’ FAC in its entirety. (Doc. 100, “Dismissal Order.”)
4 The 2022 midterm election took place on November 8, 2022.

5 The Court’s Dismissal Order described in detail the allegations Plaintiffs raised in
6 their FAC, as well as the current procedures used to administer elections in Arizona.
7 (Dismissal Order at 2–11.) Here, the Court will presume the reader’s familiarity with its
8 Dismissal Order and provide a more truncated description of Plaintiffs’ allegations, the
9 pertinent procedural history of the case, and the parties’ positions on remaining issues.

10 Broadly, Plaintiffs alleged that the electronic voting machines certified for use in
11 Arizona, including optical scanners and ballot marking devices (“BMDs”), are “potentially
12 unsecure, lack adequate audit capacity, fail to meet minimum statutory requirements, and
13 deprive voters of the right to have their votes counted and reported in an accurate, auditable,
14 legal, and transparent process.” (FAC ¶ 23.) Plaintiffs alleged that the machines are “rife”
15 with cybersecurity vulnerabilities and allow for unauthorized persons to manipulate the
16 reported vote counts in an election and potentially change the winner. (*See, e.g., id.*
17 ¶¶ 12-13, 73–75, 77, 81–82, 108–12, 125–34, 139.) Plaintiffs claimed that Arizona’s audit
18 regime is insufficient to negate these vulnerabilities and that the only way to overcome the
19 security issues they identify is “for the Court to Order, an election conducted by paper
20 ballot, as an alternative to the current framework.” (*Id.* ¶¶ 144–53.) Plaintiffs requested that
21 the Court implement certain procedures, including the use of paper ballots and a live-
22 streamed hand-count of all ballots cast. (*Id.* ¶ 153.) Plaintiffs maintained that the Cyber
23 Ninjas’ hand count of two contests in the 2020 general election in Maricopa County offers
24 “a proof-of-concept and a superior alternative to relying on corruptible electronic voting
25 systems.” (*Id.* ¶ 155.)

26 In a letter dated May 20, 2022, counsel for the Maricopa County Defendants notified
27 Plaintiffs’ counsel that this lawsuit was frivolous. (Doc. 97-1.) Counsel advised that unless
28 Plaintiffs voluntarily dismissed their suit, counsel intended to file a motion to dismiss

1 pursuant to Federal Rule of Civil Procedure 12(b)(6) and a motion for sanctions pursuant
2 to Rule 11. (*Id.*) The Maricopa County Defendants filed a Motion to Dismiss Plaintiffs’
3 FAC on June 7, 2022 (Doc. 27). Defendant Arizona Secretary of State Katie Hobbs (“the
4 Secretary”) joined the Maricopa County Defendants’ motion and filed her own Motion to
5 Dismiss on June 8, 2022 (Doc. 45).

6 On June 8, 2022, nearly seven weeks after filing their initial Complaint (Doc. 1),
7 Plaintiffs lodged a Motion for Preliminary Injunction (Doc. 50, “MPI”), which the Court
8 ordered filed on June 15, 2022 (Doc. 49). In their MPI, Plaintiffs requested that the Court
9 “enter a preliminary injunction barring Defendants from using computerized equipment to
10 administer the collection, storage, counting, and tabulation of votes in any election until
11 such time that the propriety of a permanent injunction is determined.” (MPI at 2.) Plaintiffs
12 filed multiple declarations and exhibits in support of their MPI (Docs. 33–44).

13 On July 21, 2022, the Court held a hearing at which the parties presented witness
14 testimony and the Court heard argument on Plaintiffs’ MPI and Defendants’ Motions to
15 Dismiss. (Doc. 98, Transcript of Proceedings (“Tr.”).) On August 26, 2022, the Court
16 granted Defendants’ Motions to Dismiss, denied as moot Plaintiffs’ MPI, and dismissed
17 Plaintiffs’ FAC in its entirety. (Dismissal Order at 13–21.)

18 The Maricopa County Defendants now move for sanctions against Plaintiffs and
19 their counsel under Rule 11 and 28 U.S.C § 1927. Broadly, Defendants argue that Plaintiffs
20 and their counsel made numerous false allegations about Arizona elections in their FAC
21 and MPI, that Plaintiffs’ claims are frivolous, and that they pursued this case for the
22 improper purpose of undermining confidence in elections and furthering their political
23 campaigns. (Mot. at 1–5, 7–12.) Plaintiffs oppose Defendants’ motion and argue that
24 sanctions cannot be imposed because their claims are meritorious and their factual
25 contentions are well-founded. (Resp. at 1–17.)

26

27

28

1 **II. LEGAL STANDARDS**

2 **A. Federal Rule of Civil Procedure 11**

3 Rule 11(b) provides, in relevant part:

4 By presenting to the court a pleading, written motion, or other paper—
5 whether by signing, filing, submitting, or later advocating it—an attorney or
6 unrepresented party certifies that to the best of the person’s knowledge,
7 information, and belief, formed after an inquiry reasonable under the
8 circumstances:

9 (1) it is not being presented for any improper purpose, such as to harass,
10 cause unnecessary delay, or needlessly increase the cost of litigation;

11 (2) the claims, defenses, and other legal contentions are warranted by
12 existing law or by a nonfrivolous argument for extending, modifying, or
13 reversing existing law or for establishing new law; [and]

14 (3) the factual contentions have evidentiary support or, if specifically so
15 identified, will likely have evidentiary support after a reasonable opportunity
16 for further investigation or discovery.

17 Rule 11(c)(1) provides: “If, after notice and a reasonable opportunity to respond, the court
18 determines that Rule 11(b) has been violated, the court may impose an appropriate sanction
19 on any attorney, law firm, or party that violated the rule or is responsible for the violation.”
20 However, “[t]he court must not impose a monetary sanction . . . against a represented party
21 for violating Rule 11(b)(2).” Fed. R. Civ. P. 11(c)(5)(A).

22 Applying Rule 11 “requires sensitivity to two competing considerations.” *United*
23 *Nat’l Ins. Co. v. R&D Latex Corp.*, 242 F.3d 1102, 1115 (9th Cir. 2001). “On the one hand,
24 . . . on occasion attorneys engage in litigation tactics so vexatious as to be unjustifiable
25 even within the broad bounds of our adversarial system, and . . . neither the other parties
26 nor the courts should have to abide such behavior or waste time and money coping with
27 it.” *Id.* Thus, “the central purpose of Rule 11 is to deter baseless filings.” *Cooter & Gell v.*
28 *Hartmarx Corp.*, 496 U.S. 384, 393 (1990). “On the other hand, . . . our system of litigation
is an adversary one, and . . . presenting the facts and law as favorably as fairly possible in
favor of one’s client is the nub of the lawyer’s task.” *United Nat’l Ins. Co.*, 242 F.3d at

1 1115. Sanctions therefore should be imposed “only in the most egregious situations, lest
2 lawyers be deterred from vigorous representation of their clients.” *Id.* (citation omitted).

3 Where “a complaint is the primary focus of a Rule 11 proceeding, a district court
4 must conduct a two-prong inquiry to determine (1) whether the complaint is legally or
5 factually baseless from an objective perspective, and (2) if the attorney has conducted a
6 reasonable and competent inquiry before signing and filing it.” *Holgate v. Baldwin*,
7 425 F.3d 671, 676 (9th Cir. 2005) (quoting *Christian v. Mattel, Inc.*, 286 F.3d 1118, 1127
8 (9th Cir. 2002)). The complaint need not be wholly baseless to be sanctionable: A partially
9 supported, partially unsupported filing may still be sanctionable. *See Townsend v. Holman*
10 *Consulting Corp.*, 929 F.2d 1358, 1362–65 (9th Cir. 1990) (“The relation of the allegedly
11 frivolous claim to the pleading as a whole is thus a relevant factor, but the mere existence
12 of one non-frivolous claim is not dispositive. . . .”). Nor does a subjective good faith belief
13 provide safe harbor. Rule 11’s objective standard eliminates the “empty-head pure-heart”
14 justification for frivolous arguments. *Smith v. Rocks*, 31 F.3d 1478, 1488 (9th Cir. 1994).

15 In assessing the pre-filing inquiry required under Rule 11, the court’s task is to
16 determine “whether an attorney, after conducting an objectively reasonable inquiry into the
17 facts and law, would have found the complaint to be well-founded.” *Holgate*, 425 F.3d at
18 677 (citation omitted). The court must consider “all the circumstances of a case,” *Cooter*,
19 496 U.S. at 401, focusing on the information available when the paper is filed. *See Golden*
20 *Eagle Dist. Corp. v. Burroughs Corp.*, 801 F.2d 1531, 1538 (9th Cir. 1986). Courts
21 consider factors including time constraints and deadlines, the complexity of the subject
22 matter and the party’s familiarity with it, and the ease of access to the requisite information.
23 *See CG Int’l Co. v. Rochem Int’l, Inc., USA*, 659 F.3d 53, 63 (1st Cir. 2011); *Garr v. U.S.*
24 *Healthcare, Inc.*, 22 F.3d 1274, 1279 (3d Cir. 1994); *Townsend*, 929 F.2d at 1364.

25 **B. 28 U.S.C. § 1927**

26 Section 1927 provides: “Any attorney . . . who so multiplies the proceedings in any
27 case unreasonably and vexatiously may be required by the court to satisfy personally the
28 excess costs, expenses, and attorneys’ fees reasonably incurred because of such conduct.”

1 In other words, the statute “authorizes the imposition of sanctions against any lawyer who
2 wrongfully proliferates litigation proceedings once a case has commenced.” *Pac. Harbor*
3 *Capital, Inc. v. Carnival Air Lines, Inc.*, 210 F.3d 1112, 1117 (9th Cir. 2000).

4 “Sanctions pursuant to section 1927 must be supported by a finding of subjective
5 bad faith.” *Blixseth v. Yellowstone Mtn. Club, LLC*, 796 F.3d 1004, 1008 (9th Cir. 2015)
6 (quoting *New Alaska Dev. Corp. v. Guetschow*, 869 F.2d 1298, 1306 (9th Cir. 1989)). “Bad
7 faith is present when an attorney knowingly or recklessly raises a frivolous argument or
8 argues a meritorious claim for the purpose of harassing an opponent.” *Id.* at 1007; *see also*
9 *Fink v. Gomez*, 239 F.3d 989, 993 (9th Cir. 2001) (“[R]ecklessness suffices for section
10 1927.”). Sanctions based on recklessness must be accompanied by a finding that the
11 objectionable conduct is frivolous or was intended to harass. *In re Keegan Mgmt. Co., Secs.*
12 *Litig.*, 78 F.3d 431, 436 (9th Cir. 1996). Section 1927, like Rule 11, is an extraordinary
13 remedy that courts should exercise with caution. *Id.* at 437.¹

14 **III. ANALYSIS**

15 **A. Rule 11**

16 The Maricopa County Defendants argue that Rule 11 sanctions are warranted
17 against Plaintiffs and their counsel because they made false allegations in violation of Rule
18 11(b)(3), asserted untenable and unsupported claims for relief in violation of Rules 11(b)(2)
19 and 11(b)(3), and brought this case for an improper purpose in violation of Rule 11(b)(1).
20 (Mot. at 1, 7–11.) The Court assesses these arguments in turn. For the purposes of its
21 analysis in this section, the Court uses the term “Plaintiffs” generally, without yet deciding
22 whether Plaintiffs or their counsel, or both, are responsible for any violations of Rule 11.
23
24
25

26 ¹ In addition to its authority under Rule 11 and 28 U.S.C. § 1927, the Court possesses
27 inherent authority to sanction conduct “which abuses the judicial process.” *Chambers v.*
28 *NASCO, Inc.*, 501 U.S. 32, 44–45 (1991). The Maricopa County Defendants have not
invoked the Court’s inherent authority, which the Court finds unnecessary to raise *sua*
sponte in light of its rulings under Rule 11 and Section 1927.

1 **1. Allegations Regarding the Use of Paper Ballots**

2 The Maricopa County Defendants argue that Plaintiffs made false allegations and
3 representations that Arizona voters do not vote by hand on paper ballots. (Mot. at 1, 2–4,
4 8.)² This is an important issue, which the Court discussed in detail in its Dismissal Order:

5 When the time to vote arrives, every Arizona voter casts a ballot by hand, on
6 paper. This is the law. *See* A.R.S. §§ 16-462 (primary election ballots “shall
7 be printed”), 16-468(2) (“Ballots shall be printed in plain clear type in black
8 ink, and for a general election, on clear white materials”), 16-502 (general
9 election ballots “shall be printed with black ink on white paper”). Arizona’s
10 statutes carve out one exception to this rule—voters with disabilities may
11 vote on “accessible voting devices” (sometimes referred to as “ballot
12 marking devices,” or “BMDs”), but these devices still must produce a paper
13 ballot or voter verifiable paper audit trail, which the voter can review to
14 confirm that the machine correctly marked his or her choices, and which can
be used in the event of an audit. 7 A.R.S. §§ 16-442.01; § 16-446(B)(7); 2019
[Elections Procedures Manual] at 80. . . . In the 2020 general election,
2,089,563 ballots were cast in Maricopa County, and only 453 of those were
cast using an accessible voting device. (Tr. 174:24–175:4.)

15 (Dismissal Order at 8–9.) In short, it cannot be disputed that Arizona already requires and
16 uses paper ballots. Allegations to the contrary are simply false.

17 Plaintiffs argue that they never alleged that Arizona does not use paper ballots.
18 (Resp. at 7–9.) In fact, they contend that the FAC either “presumes that Arizona uses paper
19 ballots” (*id.* at 8), or “implicitly acknowledges that Arizona uses paper ballots.” (*Id.* at 9.)
20 And they urge the issue is immaterial in any event because the use of paper ballots has no
21 effect on the substance of their claims, which they say focus on “prohibition of the counting
22 and tabulation of ballots using ‘centralized machine-counting or computerized optical
23 scanners.’” (*Id.* at 8–9, citing FAC ¶¶ 14–15, 57, 67–68, 154, 167, 170, 174.)

24 _____
25 ² Plaintiffs fault the Maricopa County Defendants for failing to cite to the allegations that
26 the Defendants contend to be false. (Resp. at 7, 9, 10, 14–15.) While it is true that the
27 Maricopa County Defendants do not provide such citations in the “Legal Argument”
28 section of their Motion, they provide citations to the FAC and MPI in a preceding section
titled “Plaintiffs’ false allegations and misleading ‘evidence.’” (Mot. at 2–5.) Plaintiffs
responded in detail to these citations in their Response. (Resp. at 7–15.) Thus, the Motion
sufficiently “describe[d] the specific conduct that allegedly violates Rule 11(b)” such that
Plaintiffs had and were afforded sufficient “notice and a reasonable opportunity to
respond.” *See* Fed. R. Civ. P. 11(c)(1), (2).

1 These statements are wrong. The FAC did not presume that Arizona uses paper
2 ballots and, in fact, alleged and implied the contrary. This is clear from the outset.
3 Paragraph 7 of the FAC summarizes the case:

4 Through this Action, Plaintiffs seek an Order that Defendants *collect and*
5 *count* votes through a constitutionally acceptable process, which relies on
6 tried and true precepts that mandates [sic] integrity and transparency. *This*
7 *includes votes cast by hand on verifiable paper ballots that maintains voter*
8 *anonymity*; votes counted by human beings, not by machines; and votes
9 counted with transparency, and in a fashion observable to the public.

10 (FAC ¶ 7 (emphasis added).) Paragraph 153 is more explicit, stating that “Plaintiffs seek
11 for the Court to Order, an election conducted by paper ballot, as an alternative to the current
12 framework.” (*Id.* ¶ 153.) An “alternative” framework is necessarily one not currently used.

13 Plaintiffs argue that “none of these paragraphs say that Arizona does not use paper
14 ballots.” (Resp. at 7–8.) That is true only in the most facile sense. A more reasonable
15 reading of these paragraphs—the only reasonable reading—is that Plaintiffs requested that
16 the Court order Arizona to do something that they contend it is not currently doing: to use
17 paper ballots. Moreover, even if Plaintiffs’ characterization of these paragraphs were
18 correct, it would only serve to establish that a central component of Plaintiffs’ request for
19 injunctive relief—requiring Arizona to use paper ballots—was entirely frivolous because
20 Defendants are already doing what Plaintiffs want them to do.

21 There is more. Paragraphs 58 to 60 of the FAC raise concerns regarding Arizona’s
22 purported move from an “auditable paper-based system” to a “computer-based system”:

23 58. Prior to 2002, most states, including Arizona, conducted their
24 elections overwhelmingly using relatively secure, reliable, and auditable
25 paper-based systems.

26 59. After the recount of the 2000 presidential election in Florida
27 and the ensuing *Bush v. Gore* decision, Congress passed the Help America
28 Vote Act in 2002. In so doing, Congress opened the proverbial spigot.
Billions of federal dollars were spent to move states, including Arizona, from
paper-based voting systems to electronic, computer-based systems.

 60. Since 2002, elections throughout the United States have
increasingly and largely been conducted using a handful of computer-based
election management systems. These systems are created, maintained, and

1 administered by a small number of companies having little to no transparency
2 to the public, producing results that are far more difficult to audit than paper-
3 based systems, and lack any meaningful federal standards or security
4 requirements beyond what individual states may choose to certify. Leaders
5 of both major parties have expressed concern about this lack of transparency,
6 analysis and accountability.

7 (FAC ¶¶ 58–60.) Plaintiffs argue that “in the context of the full Complaint, the[se]
8 allegation[s] refer[] to the systems used to count and tabulate votes.” (Resp. at 8.) Not so.
9 The section that follows these introductory paragraphs includes numerous allegations about
10 the vulnerabilities of machines by which voters cast ballots, including direct-recording
11 electronic voting machines (“DREs”) and ballot marking devices (“BMDs”), not only those
12 which count and tabulate votes. (*See, e.g.*, FAC ¶¶ 68, 77, 78, 84, 102, 104, 139.)

13 More fundamentally, a move from an “auditable paper-based voting system” to an
14 “electronic, computer-based system” more than implies a transition away from paper
15 ballots. Put differently, a system that uses paper ballots for recording votes and electronic
16 machines for tabulating them remains a “paper-based voting system.” *See* U.S. Election
17 Assistance Commission Glossary of Terms Database, <https://www.eac.gov/glossary/p>
18 (defining “Paper-Based Voting System” as a “voting system that records votes, counts
19 votes, and tabulates the vote count, using one or more ballot cards or paper ballots”).
20 Evidence submitted by Plaintiffs describes Dominion’s DVS 5.5-B voting system, which
21 is used in Maricopa County and features prominently in Plaintiffs’ allegations, as a “paper-
22 based optical scan voting system with a hybrid paper/DRE option.” (Doc. 42-1, Decl. of
23 Andrew D. Parker, Ex. C at 1.) Thus, contrary to Plaintiffs’ allegations, Arizona’s voting
24 system remains paper based. If it were otherwise, the Cyber Ninjas would not have been
25 able to conduct the audit of paper ballots Plaintiffs allege to be a “proof-of-concept” for a
26 full hand count. (FAC ¶¶ 70, 155.)

27 The section of the FAC titled “Imminent Injury” also contains allegations that
28 Arizona voters, including Plaintiffs, cast their ballots by electronic voting machines.
Paragraph 168 alleges that “Plaintiff Lake intends to vote in the Midterm Election in

1 Arizona. To do so, she will be required to cast her vote, and have her vote counted, through
2 electronic voting systems.” (FAC ¶ 168.) Paragraph 171 makes the same allegation as to
3 Plaintiff Finchem. (*Id.* ¶ 171.) These assertions are wrong: Plaintiffs are not required under
4 Arizona’s current procedures to “cast [their] vote[s]” “through electronic voting systems.”³
5 Indeed, Defendants have submitted evidence indicating Plaintiffs themselves have voted
6 on paper ballots for nearly twenty years. (Doc. 29-16, Lake and Finchem Voter Files.)⁴

7 Plaintiffs are wrong that the FAC presumes that Arizona uses paper ballots because
8 the FAC attacks Arizona’s use of optical scanners. (Resp. at 8, 9.) In fact, the FAC also
9 attacks the use of “electronic voting machines” and “electronic voting systems,” which are
10 conspicuously broader terms than “optical scanners.” (*See, e.g.*, FAC ¶¶ 1, 2, 4, 5, 10, 17,
11 24–28, 30–34, 57–61, 69, 72, 74, 76, 84, 89, 90, 92, 102, 117, 125, 144, 152.) Plaintiffs’
12 expert, Douglas Logan, testified that these terms broadly “refer to any computerized
13 devices or equipment utilized to cast, print, count, tabulate, process, and/or store ballot
14 images and/or election results.” (Doc. 39, Decl. of Douglas Logan ¶ 15.) Using these
15 broader terms allowed Plaintiffs to misleadingly analogize the machines used in Arizona
16 to those used in other jurisdictions, including machines at issue in the *Curling v.*
17 *Raffensperger* case in the Northern District of Georgia. (*See, e.g.*, FAC ¶¶ 4, 81–84, 139,
18 146.) The FAC cited to the *Curling* court’s assessment that electronic voting machines
19 were vulnerable to manipulation or interference, quoting the court’s warning that “this is
20 not a question of ‘might this actually ever happen?’—but ‘when it will happen.’” (*Id.* ¶ 84.)
21 However, as the Court previously noted, the *Curling* case is nothing like this one, in part

22 ³ The Maricopa County Defendants did not cite Paragraphs 168 and 171 in their Motion.
23 (*See* Mot. at 2–4, 8.) Thus, there is at the least the possibility of an issue whether Plaintiffs
24 were given sufficient notice that these paragraphs were potentially sanctionable. Out of an
25 abundance of caution, the Court refrains from considering these paragraphs to be
sanctionable as false allegations regarding Arizona’s use of paper ballots. However, the
Court considers them for the purposes of evaluating the arguments Plaintiffs make in their
Response generally characterizing the FAC’s allegations.

26 ⁴ On June 7, 2022, the Maricopa County Defendants filed a Motion for Judicial Notice
27 (Doc. 29), in which they requested the Court to take judicial notice of certain government
28 documents. (Docs. 29-2—29-18.) In its Dismissal Order, the Court granted the Motion—
which Plaintiffs partially opposed—only as to the government documents referenced in
that Order. (Dismissal Order at 7 n.5.) The Court now reconsiders and grants the Motion
as to the additional government documents referenced in this Order.

1 because Arizona, unlike Georgia, uses paper ballots. (*See* Dismissal Order at 8 n.7, 14–15.)
2 Indeed, in the passage Plaintiffs quoted in the FAC, the *Curling* court was describing risks
3 posed to BMDs—not optical scanners—and gave the quoted warning in the context of
4 denying a request to replace Georgia’s mandatory BMD system with “a statewide hand-
5 marked paper ballot system”—the kind of system that Arizona already uses. *See* 493 F.
6 Supp. 3d 1264, 1341–42 (N.D. Ga. 2020).

7 Similarly, the FAC cited to testimony before the Senate Rules and Administration
8 Committee by Dara Lindenbaum, then the nominee for Federal Elections Commissioner,
9 about allegations that “voting machines were used to illegally switch votes from one
10 candidate to another during the 2018 election in Georgia.” (FAC ¶ 102 & n.21.) However,
11 in the video testimony linked in the FAC, Ms. Lindenbaum testified that these allegations
12 concerned “DRE machines with no paper trail.” *See* Forbes Breaking News, “I’m a Little
13 Bit Puzzled By That Answer’: Cruz Grills FEC Nominee On Stacey Abrams’ Concession,”
14 YouTube (Apr. 7, 2022), https://www.youtube.com/watch?v=wCPLL_D_spc, at 2:47–
15 3:37. As noted, unlike the systems at issue in Georgia, Arizona’s machines produce a voter-
16 verifiable paper audit trail even as to those few votes cast electronically.

17 Thus, Plaintiffs’ argument that the FAC merely “attacks Arizona’s use of optical
18 scanners to count votes” (Resp. at 8) is incorrect. Not only did the FAC use the broader
19 terms “electronic voting machines” and “electronic voting systems” in misleadingly
20 analogizing to machines used in other jurisdictions; it specifically attacked the use of both
21 “optical scanners and ballot marking devices.” (FAC ¶ 23.) But the overwhelming majority
22 of Arizona voters—99.98% of voters in the 2020 general elections in Maricopa County,
23 for example—do not use BMDs to cast their votes. (Tr. 174:24–175:7.) The FAC variously
24 alleged that “some” (FAC ¶¶ 16, 57) or “many” Arizona voters cast their votes use BMDs.
25 (*Id.* ¶¶ 68, 167.) While it is true, as Plaintiffs note (Resp. at 8), that these allegations may
26 be reasonably read to imply that other Arizona voters use paper ballots, they did not cure
27 the FAC’s other allegations and overarching implication that Arizona does not have an
28 auditable, paper-ballot based voting system.

1 The Maricopa County Defendants contend that Plaintiffs continued to make false
2 representations about the use of paper ballots in their MPI. (Mot. at 3–4, citing MPI at 2;
3 *see also* Mot. at 8.)⁵ An introductory paragraph of the MPI reads:

4 Experience has now shown the move to *computerized voting* in Arizona was
5 a mistake—an unnecessary, unsecure change that opened election results to
6 manipulation by unauthorized persons. This is not a partisan issue. Experts
7 across the political spectrum have long sounded the alarm about the inherent
8 insecurity and lack of transparency in *computerized voting systems* such as
9 those used in Arizona. It is time to reverse this mistake. The right to vote is
10 constitutionally guaranteed. *Computerized voting systems* leave an open door
for votes to be changed, deleted, or fabricated in violation of constitutional
requirements. *A return to the tried-and-true paper ballots of the past—and*
of the present, in countries like France, Taiwan, and Israel—is necessary.

11 (MPI at 2 (emphasis added).) In their Response, Plaintiffs argue that their use of the term
12 “computerized voting” is accurate because “[Arizona’s] is a computerized voting system,
13 notwithstanding the role that paper ballots play in it, because the *outcomes of the election*
14 *contests* are determined by what computers *do* with the paper ballots.” (Resp. at 14
15 (emphasis in original).) Even viewing the term “computerized voting” in isolation, the
16 Court is not persuaded. In any event, the MPI does not use the term in isolation. The
17 preceding paragraph contrasts “electronic, computerized voting systems” with the prior
18 practice by which “American voters recorded their votes by hand on paper ballots that were
19 counted by human beings.” (MPI at 1.) Moreover, the MPI directly states that a “return to
20 . . . tried-and-true paper ballots . . . is necessary” (*id.* at 2), clearly implying that Arizona
21 does not currently use paper ballots. If it did, then this statement would be meaningless and
22 therefore a central component of Plaintiffs’ request for injunctive relief would be frivolous.

23 Finally, Plaintiffs argue that any allegations or implications that Arizona does not
24 use paper ballots are not sanctionable because the use of paper ballots is immaterial to their

25 ⁵ In their Response, Plaintiffs do not specifically address the Maricopa County Defendants’
26 arguments about these allegedly false statements in the MPI. (*See* Resp. at 7–9.) As noted
27 in Footnote 2, *supra*, Plaintiffs fault the Maricopa County Defendants for failing to cite to
28 their allegedly false statements. (*Id.* at 7, 9, 10, 12, 14–15.) But the Maricopa County
Defendants provided citations to the allegedly false statements in the MPI in the section of
their Motion titled “Plaintiffs’ false allegations and misleading ‘evidence.’” (Mot. at 2–4,
citing MPI at 2.) The Court therefore considers whether the cited statements in the MPI are
sanctionable, notwithstanding Plaintiffs’ failure to address them in their Response.

1 claims. (Resp. at 8–9.) Plaintiffs cite, for example, to the Second Circuit’s opinion in *Kiobel*
2 *v. Millson* for the proposition that “even literally false minor overstatement error ‘does not
3 violate Rule 11’ where ‘pleading as a whole remains well grounded in fact.’” (*Id.* at 8,
4 citing 592 F.3d 78, 83 (2d Cir. 2010) (quotation omitted).) But the Ninth Circuit long ago
5 expressly rejected the “pleading-as-a-whole” rule. *See Townsend*, 929 F.2d at 1362–65
6 (overruling *Murphy v. Bus. Cards Tomorrow, Inc.*, 854 F.2d 1202, 1205 (9th Cir. 1988)).

7 Instead, the Ninth Circuit instructs that courts may consider the relation of the
8 unsupported portion of the complaint to the pleading as a whole. *See Townsend*, 929 F.2d
9 at 1363–65. Here, Plaintiffs’ misrepresentations about Arizona’s use of paper ballots
10 played a central role in the purported basis for Plaintiffs’ claims. By alleging and implying
11 that Arizona does not currently have an auditable paper-ballot system, Plaintiffs set up a
12 strawman, constructed in substantial part based on the *Curling* case and concerns about
13 voting machines in other jurisdictions. But the strawman was just that. Arizona already
14 follows the course to “eliminate or greatly mitigate” the risks of manipulation and
15 interference that Prof. Halderman recommended in the *Curling* litigation: It uses paper
16 ballots and reserves BMDs for the small number of voters who need or request them. (*See*
17 Dismissal Order at 8–9 & n.7, quoting Halderman Dec. 33, Doc. 1304-3, *Curling v.*
18 *Raffensperger*, No. 1:17-CV-2989-AT (N.D. Ga. Feb. 3, 2022).) And again, even those
19 BMD-assisted voters produce a paper ballot or voter-verifiable paper audit trail. (*Id.*)⁶

20
21 ⁶ On the day of the 2022 midterm election, Maricopa County officials stated that equipment
22 problems affected at least 30% of the County’s voting centers. Robert Anglen *et al.*, “It all
23 turns on Maricopa County: Takeaways from a day of glitches, conspiracies and a lawsuit,”
24 *The Arizona Republic* (Nov. 9, 2022),
25 [https://www.azcentral.com/story/news/politics/elections/2022/11/09/maricopa-county-
26 election-glitches-conspiracies-and-lawsuit/8312190001/](https://www.azcentral.com/story/news/politics/elections/2022/11/09/maricopa-county-election-glitches-conspiracies-and-lawsuit/8312190001/). In a video, Defendant Gates,
27 Chairman of the Maricopa County Board of Supervisors, stated that the County would
28 proceed to tabulate at the County’s Ballot Tabulation Center the ballots that the tabulators at
the voting centers were unable to read. *Id.* According to press reports, officials with the U.S.
Cybersecurity and Infrastructure Security Agency (“CISA”) said that CISA saw no specific
or credible threat to disrupt election infrastructure or election day operations, that the issue
in Maricopa County appeared to be a fairly routine technical glitch, and that Arizona’s use
of paper ballots would provide opportunities to verify—and audit—the votes if necessary.
Id. The Court’s observation regarding these day-of-vote issues would seem to underscore the
significance of Arizona’s use of auditable paper ballots. However, this observation plays no
part in the Court’s decisions herein.

2. Allegations Regarding Testing of Arizona’s Election Equipment

The Maricopa County Defendants argue that the FAC made false allegations that Arizona’s tabulation machines are not independently tested by experts. (Mot. at 2–3, citing FAC ¶¶ 20, 57, 69; *see also* Mot. at 8.) Plaintiffs respond that none of the cited paragraphs in the FAC say that Arizona does not test its tabulation machines. (Resp. at 9–10.) But they nonetheless further question whether such testing took place, contending that “[a] statutory requirement of testing does not prove that testing actually occurred.” (*Id.*) Finally, they dispute that the testing and certification procedures used in Arizona “constitute neutral, expert analysis,” and therefore argue that the FAC’s allegations merely reflect a reasonable difference of opinion between the parties that is not sanctionable under Rule 11. (*Id.*)

Of the three paragraphs cited by Defendants on this point, the Court agrees with Plaintiffs that Paragraph 69 is not sanctionable because it arguably refers to Dominion’s purported failure to subject its machines to testing, rather than Arizona’s failure to test its machines. The other two are not so ambiguous, however. Paragraph 20 alleges that the Secretary’s “certification of the Dominion Democracy Suite 5.5b voting system, as well as its component parts, was improper, *absent objective evaluation.*” (FAC ¶ 20 (emphasis added).) Paragraph 57 alleges that “Arizona intends to rely on electronic voting systems to record some votes and to tabulate *all* votes cast in the State of Arizona in the 2022 Midterm Election, *without disclosing the systems and subjecting them to neutral, expert analysis.*” (*Id.* ¶ 57 (first emphasis in original and second emphasis added).) These are allegations that Arizona’s electronic voting systems have not been subjected to objective evaluation or neutral, expert analysis. And they are wrong. As the Court previously discussed, Arizona’s equipment undergoes thorough testing by independent, neutral experts with the Secretary of State’s Certification Committee and a testing laboratory accredited by the Election Assistance Commission (“EAC”).⁷ (*See* Dismissal Order at 6–7 and documents cited

⁷ The EAC is an independent federal agency that was established by the Help America Vote Act of 2002 and is charged with providing for “the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories.” 52 U.S.C. § 20971(a)(1).

1 therein.) For example, Maricopa County’s equipment was tested by Pro V&V, an EAC-
2 accredited testing laboratory, and tested—in public—by the Secretary of State’s
3 Equipment Certification Committee. (*See id.*) This is in addition to the County’s testing of
4 its equipment and the audits of vote-tabulation results. (*See id.* at 7–10 & n.6.)⁸

5 In their Response, Plaintiffs criticize the process by which Arizona’s equipment is
6 tested and argue that the parties may reasonably dispute whether the process constitutes
7 “objective evaluation” or “neutral, expert analysis.” (Resp. at 10.) At bottom, however,
8 Plaintiffs’ concerns are about the sufficiency and reliability of Arizona’s testing process.
9 But the FAC does not merely allege that testing of Arizona’s equipment is insufficient or
10 unreliable; it alleges that the equipment has not been subjected to objective evaluation or
11 neutral, expert analysis, which is not true. Plaintiffs and their experts may be entitled to
12 opine about the sufficiency of the testing that Arizona’s machines undergo, but they are
13 not entitled to allege that no such testing takes place.

14 **3. Allegations Regarding the Lack of Vote-Verifying Audits**

15 The Maricopa County Defendants argue that Plaintiffs’ FAC falsely alleged that
16 Arizona’s tabulation results are not subject to vote-verifying audits. (Mot. at 2–3, citing
17 FAC ¶¶ 23, 72, 144–52; *see also* Mot. at 8.) Plaintiffs respond that Defendants
18 mischaracterize the FAC. (Resp. at 10–12.) They argue that the FAC does not allege that
19 Arizona does not conduct audits; it contests the sufficiency of the audits. (*Id.*)

20 While this issue presents a closer call, the Court agrees with Plaintiffs that the FAC
21 did not directly allege that Arizona’s tabulation results are not audited. Paragraphs 23 and
22 72 allege that Arizona’s voting machines cannot deliver accurate results, and therefore
23 comport with constitutional and statutory requirements, “without objective evaluation,” in
24 part because the machines “lack adequate audit capacity.” (FAC ¶¶ 23, 72.) On their own,
25 these paragraphs may be reasonably read as an assertion that Arizona’s tabulation results
26 are not objectively evaluated, which, as discussed, is not true. However, Paragraphs 144 to

27 _____
28 ⁸ As to whether testing in fact occurred, Plaintiffs’ expert, Douglas Logan, testified he was aware that Arizona’s system was EAC certified and subjected to logic and accuracy testing, though he criticized the sufficiency and reliability of those processes. (Tr. 62:11—65:13.)

1 152 subsequently allege that Arizona’s existing audit regime is insufficient, necessarily
2 implying that such a regime exists. (*Id.* ¶¶ 144–52.)

3 **4. Allegations Regarding the Cyber Ninjas’ Hand Count in**
4 **Maricopa County**

5 Defendants label as untrue the FAC’s “allegation that “[t]he recent hand count in
6 Maricopa County, the second largest voting jurisdiction in the United States, offers
7 Defendant Hobbs a proof-of-concept and a superior alternative to relying on corruptible
8 electronic voting systems.” (Mot. at 3, quoting FAC ¶ 155; *see also* Mot. at 8.) Plaintiffs
9 counter that whether the Cyber Ninjas’ hand count can be characterized as a “proof-of-
10 concept and a superior alternative” is a matter of judgment. (Resp. at 12–13.) They argue
11 that the word “superior” should be interpreted as a measure of “transparency” rather than
12 “speed or cost,” and that the Cyber Ninjas “showed a hand count can be done; it does not
13 show the optimized method of doing it.” (*Id.*)

14 Setting aside issues concerning the reliability of the Cyber Ninjas’ audit, it strains
15 credulity to characterize the hand count as a proof-of-concept that a full hand count is
16 “feasible”—let alone a “superior alternative.” Arizona law requires that county boards of
17 supervisors canvass general elections within twenty days after the election. A.R.S.
18 § 16-642(A). Mr. Logan testified that in the Cyber Ninjas’ hand count, it took roughly
19 2,000 people more than two-and-a-half months to hand count only two (out of several
20 dozen) contests on each ballot in only one of Arizona’s fifteen counties. (Tr. 71:20–74:4.)
21 Scott Jarrett, the co-director of the Maricopa County Elections Department, estimated that
22 a full hand count for the 2022 midterm election in Maricopa County alone would require
23 hiring 25,000 temporary workers and finding two million square feet of space. (Tr. 196:6–
24 198:8.) He testified that with the County’s current employees, “it would be an
25 impossibility” to have the ballots counted to perform the canvass by the twentieth day after
26 the election, as required by law. (Tr. 194:16–23.) In short, Plaintiffs’ characterizations of
27 the Cyber Ninjas’ hand count would be wholly unpersuasive to any objective reader with
28

1 an understanding of the underlying facts. Nonetheless, the Court will treat Plaintiffs’
2 incredible arguments on this point as such, rather than as false assertions of fact.

3 Defendants further assert that Plaintiffs made factual misstatements regarding
4 Cyber Ninjas’ findings that have been debunked. (Mot. at 3, citing FAC ¶¶ 70, 132, 164;
5 *see also* Mot. at 8.) But the cited portions of the FAC quote and summarize the Cyber
6 Ninjas’ report and therefore do not constitute Plaintiffs’ direct allegations, at least not in a
7 manner the Court finds sanctionable. The Court notes, however, that Plaintiffs cherry-
8 picked among the Cyber Ninjas’ findings and ignored those that undermine their claims.
9 They conspicuously failed to mention that the Cyber Ninjas’ report states that “there were
10 no substantial differences between the hand count of the ballots provided and the official
11 election canvass results for Maricopa County. This is an important finding because the
12 paper ballots are the best evidence of voter intent and there is no reliable evidence that the
13 paper ballots were altered to any material degree.” *Maricopa County Forensic Election*
14 *Audit, Volume I at 1* (Sept. 24, 2021),
15 [https://www.azsenaterepublicans.com/_files/ugd/2f3470_a91b5cd3655445b498f9acc63d](https://www.azsenaterepublicans.com/_files/ugd/2f3470_a91b5cd3655445b498f9acc63db35afd.pdf)
16 [b35afd.pdf](https://www.azsenaterepublicans.com/_files/ugd/2f3470_a91b5cd3655445b498f9acc63db35afd.pdf).

17 **5. Allegations Regarding the Internet Connectivity of Maricopa** 18 **County’s Elections Systems**

19 Defendants argue that “the entire FAC is premised on the erroneous theory that
20 machine counting of ballots is unreliable because the machines used are ‘potentially
21 susceptible to malicious manipulation that can cause incorrect counting of votes’ and these
22 alleged vulnerabilities stem from the possibility that the machines ‘can be connected to the
23 internet.’” (Mot. at 5, quoting FAC ¶¶ 26, 33; *see also* Mot. at 5, citing FAC ¶¶ 70, 132,
24 164; *see also* Mot. at 8.) Plaintiffs respond that their allegations about the internet
25 connectivity of Maricopa County’s systems are well-founded. (Resp. at 14.)

26 To support their argument, Plaintiffs cite to the testimony of their expert, Benjamin
27 Cotton, who analyzed election systems provided by Maricopa County during the Cyber
28 Ninjas’ audit. (Resp. at 14, citing Tr. 27:2–29:13.) In the cited portion of his testimony,

1 Mr. Cotton testified that he saw “actual evidence of remote log-ins into [Maricopa
2 County’s election management server].” (Tr. 27:2–7.) When asked “whether those were
3 permissible or security breach,” he responded: “The attributable log-ins—because I did see
4 some anonymous log-ins that I could not trace back to an event. The ones that I saw came
5 from the local EMS subnet, if you will, the IP address that—for the voting system.” (Tr.
6 27:8–13.) Mr. Cotton’s testimony is somewhat unclear, but to the extent it refers to the
7 findings in the Cyber Ninjas’ report that an “anonymous user” accessed Maricopa County’s
8 EMS server, the County asserted that those findings are false because “[t]hese logged
9 actions are simply part of the EMS server protocols and standard Microsoft functions.”
10 (Doc. 29-14, *Correcting the Record* at 34–35.) Mr. Cotton further testified that “each of
11 the Dell computers that were within that system did have wifi cards and that those wifi
12 cards had been registered as a network on the computing devices.” (Tr. 27:18–28:11.)
13 When asked if he was describing a “hotspot” and whether “[i]f someone gained access,
14 they could utilize the hotspot to gain access,” Mr. Cotton responded: “Sure, yeah. That
15 would give access to the Internet.” (Tr. 28:12–17.) He proceeded to give examples of
16 breaches through other air-gapped systems not used by Maricopa County. (Tr. 29:16–28:6.)

17 In March 2022, the Special Master designated by the Arizona State Senate and
18 Maricopa County to examine the County’s election network and equipment reported
19 finding “NO evidence that the routers, managed switches, or electronic devices [in
20 Maricopa County’s Ballot Tabulation Center] connected to the public Internet.” (Doc. 37,
21 Decl. of Benjamin R. Cotton, Ex. H, *Answers to Senate Questions Regarding Maricopa
22 County Election Network* (Mar. 23, 2022) at 10.) The Special Master stated that Maricopa
23 County uses an air-gapped system that “provides the necessary isolation from the public
24 Internet, and in fact is in a self-contained environment” with “no wired or wireless
25 connections in or out of the Ballot Tabulation Center,” and “[a]s such, the election network
26 and election devices cannot connect to the public Internet.” (*Id.* at 10–11.) The Special
27 Master’s findings are consistent with what the County has long maintained (*see, e.g.*,
28 Doc. 29-14, *Correcting the Record* at 36–44), and what previous audits have likewise

1 concluded. (*See, e.g.*, Doc. 29-8, SLI Compliance, *Forensic Audit Report: Dominion*
2 *Voting Systems, Democracy Suite 5.5B* at 14–16 (Feb. 23, 2021).)

3 Although Plaintiffs’ claims that Maricopa County’s systems can be or have been
4 connected to the internet are in direct contradiction to the County Defendants’ evidence
5 and the Special Master’s findings, the Court will treat them as unpersuasive arguments
6 rather than as false assertions of fact, allowing Plaintiffs the benefit of the doubt. However,
7 the Court notes that to rely on the Cyber Ninjas’ findings on this issue, without mentioning
8 in the FAC that the Special Master contradicted those findings, is misleading. Litigants are
9 entitled to raise disputed issues, but they may not misrepresent or withhold material facts
10 that refute their allegations. *See Burroughs*, 801 F.2d at 1539 (finding “no quarrel” with
11 the district court’s admonition that the “omission of critical facts” may be sanctionable
12 under Rule 11). Nonetheless, the Court does not deem this issue sanctionable here.

13 **6. Unsupported Claims Based on Speculation and Conjecture**

14 The Maricopa County Defendants argue that Plaintiffs violated Rules 11(b)(2) and
15 (b)(3) by pursuing untenable and unsupported claims based on conjecture and
16 speculation—claims that are, in a word, frivolous. (Mot. at 2, 8–9.) They point to Plaintiffs’
17 reliance on “testimony and allegations that are entirely unrelated to elections in Arizona”
18 (*id.* at 4, citing FAC ¶¶ 73–89, 125–31, 133, 134); Plaintiffs’ allegations concerning alleged
19 foreign manufacture of election machines that fail to identify specific machines or parts
20 (*id.*, citing FAC ¶¶ 90–92); and Plaintiffs’ tangential discussion of “open source”
21 technology. (*Id.*, citing FAC ¶¶ 108–24.) Defendants further cite to their Response to
22 Plaintiffs’ MPI (Doc. 57), in which they discussed Plaintiffs’ reliance on the
23 distinguishable *Curling* case (*id.* at 3–4); Plaintiffs’ use of out-of-context quotations and
24 testimony in other proceedings (*id.* at 4–5); and Plaintiffs’ reliance on a recent statement
25 from the U.S. Cybersecurity and Infrastructure Agency (“CISA”) concerning
26 vulnerabilities in a version of Dominion’s DVS 5.5 voting system that Arizona does not
27 currently use. (*Id.* at 5.) What Plaintiffs failed to allege, Defendants argue, is that Arizona’s
28

1 ballot tabulation equipment has ever been hacked or manipulated or improperly counted
2 votes—“because no such evidence exists.” (Mot. at 8.)

3 Plaintiffs counter that their claims are well-founded and meritorious. (Resp. at 1-2.)
4 They argue that the summary allegations in the FAC about the vulnerabilities of Arizona’s
5 voting machines are supported by detailed allegations which are, in turn, supported by the
6 evidentiary record on Plaintiffs’ MPI. (*Id.* at 1–4.) Plaintiffs discuss some of this evidence
7 in their Response, including a declaration by Professor Walter Daugherty (Doc. 38)
8 discussing his analysis of cast vote records from the 2020 general election in Maricopa and
9 Pima Counties. (*Id.* at 3–6.) More fundamentally, Plaintiffs argue that

10 even if no past manipulation of Arizona ballots had not been shown [sic], *an*
11 *absence of undisputed evidence that a particular harm has happened before*
12 *in a particular location does not prove that the harm cannot happen in the*
13 *future, particularly where similar events have happened elsewhere. . . . ‘It*
14 *hasn’t happened here yet’ does not prove ‘it can’t happen here.’ It is not*
sanctionable to bring an action seeking to prevent a foreseeable and likely
harm that has not yet happened here.

15 (Resp. at 5 (emphasis in original).) Because they put forth evidence from which “[i]t is
16 reasonable to infer . . . that an electronic intrusion designed to take advantage of the
17 vulnerabilities in Maricopa’s electronic system and manipulate votes is likely to occur in
18 the future,” Plaintiffs assert their claims “are meritorious, not sanctionable.” (*Id.* at 5–6.)

19 An in-depth discussion of Plaintiffs’ allegations and supporting evidence is
20 unnecessary here for the purposes of evaluating whether their claims rest on an adequate
21 legal and factual basis. Whatever weight one assigns to Plaintiffs’ evidence, an essential
22 flaw remains in their overarching theory of the case. Simply put, there are yawning gaps
23 between the factual assertions made, the harm claimed, and the ultimate relief requested.

24 Plaintiffs never put forth sufficient allegations about Arizona’s election systems—
25 let alone sufficient evidence to support any such allegations—to demonstrate a likelihood
26 that Arizonans’ votes would be incorrectly counted in the 2022 midterm election due to
27 manipulation. The Court reached this conclusion in its Dismissal Order, where it ruled that
28 Plaintiffs’ claimed injuries were too speculative to meet the injury-in-fact requirement for

1 standing under Article III. (Dismissal Order at 13–16.) *See Clapper v. Amnesty Int’l USA*,
2 568 U.S. 398, 409 (2013) (holding that a threatened injury must be “actual or imminent”
3 and “certainly impending” to confer Article III standing and that “allegations of possible
4 future injury are not sufficient”) (citations omitted). The Court explained:

5 [A] long chain of hypothetical contingencies must take place for any harm to
6 occur—(1) the specific voting equipment in Arizona must have “security
7 failures” that allow a malicious actor to manipulate vote totals; (2) such an actor
8 must actually manipulate an election; (3) Arizona’s specific procedural
9 safeguards must fail to detect the manipulation; and (4) the manipulation must
10 change the outcome of the election. (*See* Doc. 62 at 2–3.) Plaintiffs fail to
11 plausibly show that Arizona’s voting equipment even has such security failures.
12 And even if the allegations in Plaintiff’s complaint were plausible, their alleged
13 injury is not “certainly impending” as required by *Clapper*. 568 U.S. at 409.

14 (Dismissal Order at 14–15 (footnotes omitted).) The Court noted the numerous steps that
15 Defendants have taken to ensure that the alleged security failures do not exist or occur,
16 including extensive post-election audit procedures. (*Id.* at 15 nn.13, 14.)

17 At bottom, Plaintiffs’ allegations raised questions about whether Arizona’s voting
18 machines are “potentially susceptible to malicious manipulation” (FAC ¶ 33), or
19 “potentially unsecure” (*id.* ¶ 23), or have vulnerabilities that “at the very least, call into
20 question” the results they produce (*id.* ¶ 69), but they went no further. A central theory of
21 the FAC is that Arizona’s voting machines cannot legally be used “unless and until the
22 electronic voting system is made open to the public and subjected to scientific analysis by
23 objective experts *to determine whether it is secure from manipulation or intrusion.*”
24 (FAC ¶ 1 (emphasis added); *see also, e.g., id.* ¶¶ 6, 20, 23, 72.) This is speculative on its
25 face. And in any event, Plaintiffs are not constitutionally entitled to their preferred voting
26 methods. *See, e.g., Weber v. Shelley*, 347 F.3d 1101, 1106–07 (9th Cir. 2003). They had
27 the burden to plausibly allege that Arizona’s use of electronic voting systems would violate
28 their constitutional rights or federal law. They failed to do so. Indeed, they appeared to
assume the very thing they had the burden to allege and ultimately prove, alleging that
Defendants have “subject[ed] voters to cast votes on an illegal and unreliable system—a
system that must be *presumed* to be compromised and incapable of producing verifiable

1 results.” (*Id.* ¶ 181 (emphasis added).) But Plaintiffs never established any adequate factual
2 or legal basis to support such a presumption.

3 Plaintiffs sought to fill the gap between their assertions about Arizona’s voting
4 equipment and their speculative conclusions about its vulnerability with allegations that were
5 false and misleading, as the Court discussed above. The Court further agrees with the
6 Maricopa County Defendants that Plaintiffs also sought to fill this gap with assertions
7 regarding elections in other jurisdictions that provided little if any support for their claims
8 and served only to muddy the waters. For example, as discussed above, Plaintiffs heavily
9 relied on the *Curling* case in Georgia (*see, e.g.*, FAC ¶¶ 4, 81–84, 139, 146), despite the fact
10 that Arizona, unlike Georgia, uses hand-marked paper ballots. In testimony before the Senate
11 Select Committee on Intelligence—a transcript of which Plaintiffs included as an exhibit—
12 Professor Halderman responded to a question about recommended actions for safeguarding
13 elections by stating “[t]he most important things are to make sure we have votes recorded on
14 paper, paper ballots, which just cannot be changed in a cyber attack” (Doc. 43, *Russian*
15 *Interference in the 2016 U.S. Elections* at 91, S. Hrg. 115–92 (June 21, 2017).) Arizona has
16 that, and has had it all along.

17 As the Maricopa County Defendants note, Plaintiffs raised other tangential
18 allegations that provided little if any support for their claims, including vague allegations
19 about foreign manufacture of election machines (FAC ¶¶ 90–92); digressions about “open
20 source” technology (*id.* ¶¶ 117–23); and discussions of Dominion’s DVS 5.5-A BMDs (*id.*
21 ¶¶ 103–05) and CISA’s report about potential vulnerabilities of these devices (MPI at 5
22 & n.2)—which again are the *prior* versions of the since-updated devices Maricopa County
23 uses. (Doc. 57-1, First Decl. of Scott Jarrett ¶¶ 27–30.) Nor did the evidence Plaintiffs point
24 to in their Response bring their claims out of the realm of speculation. Even if this evidence
25 were sufficient to identify vulnerabilities—which the Court does not decide—it is
26 insufficient to establish a likelihood that Arizonans’ votes will not be correctly counted due
27 to manipulation of electronic voting machines.

28

1 The relief that Plaintiffs sought in this case was remarkable. Mere months away
2 from the 2022 midterm election, Plaintiffs requested, among other relief, an Order
3 “declaring it unconstitutional for any public election to be conducted using any model of
4 electronic voting system to cast or tabulate votes”; an injunction prohibiting Defendants
5 from utilizing any of their electronic voting systems; and an Order that all Arizona ballots
6 be cast on paper, by hand, and that every vote be counted, by hand, according to specific
7 procedures outlined by Plaintiffs. (FAC at 49-50; *see also id.* ¶ 153.) Setting aside that the
8 overwhelming majority of Arizona voters already cast paper ballots, the relief that
9 Plaintiffs requested in this case would have called for a massive, perhaps unprecedented
10 federal judicial intervention to overhaul Arizona’s elections procedures shortly before the
11 election. Plaintiffs bore a substantial burden to demonstrate that such an intervention was
12 constitutionally required and in the public interest. Yet they never had a factual basis or
13 legal theory that came anywhere close to meeting that burden. Underscoring just how far
14 short of that heavy burden they fell, Plaintiffs failed to show that their preferred full hand
15 count would be feasible or more accurate than Arizona’s current procedures, as the Court
16 previously discussed in denying Plaintiffs’ MPI. (*See* Dismissal Order at 2 n.1.)

17 In sum, Plaintiffs lacked an adequate factual or legal basis to support the wide-
18 ranging constitutional claims they raised or the extraordinary relief they requested.
19 Plaintiffs filled the gaps between their factual assertions, claimed injuries, and requested
20 relief with false, misleading, and speculative allegations. At its core, Plaintiffs’ FAC
21 presented mere conjectural claims of potential injuries. Rule 11 requires more. “While
22 there are many arenas—including print, television, and social media—where protestations,
23 conjecture, and speculation may be advanced, such expressions are neither permitted nor
24 welcomed in a court of law.” *King v. Whitmer*, 556 F. Supp. 3d 680, 689 (E.D. Mich. 2021).

25 **7. Failure to Conduct a Reasonable Pre-Filing Inquiry**

26 Plaintiffs had plenty of time in which to thoroughly investigate the factual and legal
27 basis for their claims. The statutory scheme that Plaintiffs sought to challenge in this case
28 has authorized Arizona’s counties to use vote-tabulation machines since at least 1966. (*See*

1 Doc. 29-15, 1966 Ariz. Sess. Laws 178–87.) The Secretary certified the Dominion DVS
2 5.5-B electronic voting systems that Plaintiffs sought to invalidate in November 2019.
3 (Doc. 29-6, Certification Letter (Nov. 5, 2019).) Further, while the subject matter of this
4 case is not simple, counsel for Plaintiffs have been involved in litigation concerning voting
5 procedures before, including litigation involving unsupported claims about electronic
6 voting machines. *See US Dominion, Inc. v. MyPillow, Inc.*, No. CV-21-0445 (CJN), 2022
7 WL 1597420, at *14 & n.11 (D.D.C. May 19, 2022) (ordering sanctions against Michael
8 Lindell and his earlier counsel, whom counsel for Plaintiffs later replaced, for filing
9 groundless and frivolous claims). As for Plaintiffs themselves, Mr. Finchem is a candidate
10 for the state’s chief election officer and Ms. Lake is a candidate for its top executive office.⁹
11 Both have apparently voted on paper ballots for nearly twenty years. (Doc. 29–15, Lake
12 and Finchem Voter Files.)

13 The circumstances of this case not only allowed for, but required, a significant pre-
14 filing inquiry. As noted, Plaintiffs’ requested relief called for a massive, late-breaking, and
15 perhaps unprecedented federal judicial intervention in Arizona’s elections. And although
16 Plaintiffs asserted that this case was “not about undoing the 2020 presidential election”
17 (FAC ¶ 8), the Court cannot ignore the dangers posed by making wide-ranging allegations
18 of vote manipulation in the current volatile political atmosphere. Indeed, the Maricopa
19 County Defendants raise troubling allegations about “the County’s witnesses and counsel
20 being confronted upon exiting the courtroom by someone who had watched the
21 proceedings, who called them ‘liars’ and ‘traitors.’” (Reply at 8.) As the court warned in
22 *King v. Whitmer*, unfounded claims about election-related misconduct “spread the narrative
23 that our election processes are rigged and our democratic institutions cannot be trusted.
24 Notably, many people have latched on to this narrative, citing as proof counsel’s
25 submissions in this case.” *King*, 556 F. Supp. 3d at 732. The Court shares this concern.

26 Plaintiffs evidently failed to conduct the factual and legal pre-filing inquiry that the
27 circumstances of this case reasonably permitted and required. The Court need not conduct

28 ⁹ At the time the Court issued this Order, the results of the 2022 midterm election have not yet been certified; thus the Court deems all persons running still to be candidates.

1 a further evidentiary inquiry to make this finding. As discussed herein, any objectively
2 reasonable investigation of this case would have led to publicly available and widely
3 circulated information contradicting Plaintiffs’ allegations and undercutting their claims.
4 Thus, Plaintiffs either failed to conduct the reasonable factual and legal inquiry required
5 under Rule 11, or they conducted such an inquiry and filed this lawsuit anyway. Either
6 way, no reasonable attorney, “after conducting an objectively reasonable inquiry into the
7 facts and law, would have found the complaint to be well-founded.” *Holgate*, 425 F.3d at
8 677 (citation omitted).

9 **8. Improper Purpose**

10 Finally, the Maricopa County Defendants argue that Plaintiffs and their counsel
11 brought this lawsuit “for the improper purpose of undermining confidence in elections and
12 to further their political campaigns.” (Mot. at 9–10.) Defendants argue that even though
13 Arizona has long used electronic voting machines, Plaintiffs waited to challenge Arizona’s
14 use of these systems until it was “politically profitable” because “they were running for
15 statewide political office, [and] a significant portion of their likely voters had become
16 erroneously convinced that the 2020 election was ‘stolen.’” (*Id.* at 9.) Defendants point to
17 statements by Plaintiff Finchem regarding his intention not to concede his election contest
18 and to require a hand count of all ballots “if there’s the slightest hint of any impropriety”—
19 statements with which Plaintiff Lake apparently agreed. (*Id.*, citing Mary Jo Pitzl, “Setting
20 up another conflict with Trump, Ducey endorses Beau Lane for Arizona secretary of state,”
21 *The Arizona Republic* (July 13, 2022),
22 [https://www.azcentral.com/story/news/politics/arizona/2022/07/13/arizona-gov-doug-](https://www.azcentral.com/story/news/politics/arizona/2022/07/13/arizona-gov-doug-ducey-endorses-beau-lane-secretary-state/10053166002/)
23 [ducey-endorses-beau-lane-secretary-state/10053166002/.](https://www.azcentral.com/story/news/politics/arizona/2022/07/13/arizona-gov-doug-ducey-endorses-beau-lane-secretary-state/10053166002/))

24 Plaintiffs respond that the evidence of improper purpose cited by the Maricopa
25 County Defendants merely shows that “Plaintiffs only recently became aware of the full
26 extent of the problems with electronic election equipment,” “genuinely believe hand
27 counting is the only reliable means of counting votes,”¹⁰ and “will not concede defeat in their

28 ¹⁰ In an election-night address posted to her Twitter account, Plaintiff Lake criticized the
“incompetency” of Arizona’s elections officials in light of the length of time it takes to

1 election contests without pursuing their rights to contest any impropriety.” (Resp. at 6.)
2 Plaintiffs further argue that their claims are not frivolous and thus not sanctionable. (*Id.*)

3 While it is a very close call, the Court finds the record as it stands insufficient to
4 compel a finding as to whether Plaintiffs brought this lawsuit for an improper purpose. The
5 Court is not inclined to further develop the record on this issue, particularly in light of its
6 findings regarding other violations of Rules 11(b)(2) and 11(b)(3), as discussed above.
7 Rule 11 confers discretion, *see Perez v. Posse Comitatus*, 373 F.3d 321, 325–26 (2d Cir.
8 2004), and it counsels restraint. *See Keegan*, 78 F.3d at 437. The deterrent goal of Rule 11
9 can be furthered in this case without conducting further inquiry into the circumstances
10 under which this lawsuit was filed.

11 It should be clear, however, that the Court does not find that Plaintiffs have acted
12 appropriately in this litigation. The Court shares the concerns expressed by other federal
13 courts about misuse of the judicial system to baselessly cast doubt on the electoral process
14 in a manner that is conspicuously consistent with the plaintiffs’ political ends. *See*
15 *O’Rourke v. Dominion Voting Systems, Inc.*, 552 F. Supp. 3d 1168, 1176 (D. Colo. 2021)
16 (“While Plaintiffs’ counsel insist that the lawsuit was not intended to challenge the election
17 or reverse the results, the effect of the allegations and relief sought would be to sow doubt
18 over the legitimacy of the [subsequent] presidency and the mechanisms of American
19 democracy (the actual systems of voting) in numerous states.”); *King*, 556 F. Supp. 3d at
20 689 (“[T]his case was never about fraud—it was about undermining the People’s faith in
21 our democracy and debasing the judicial process to do so.”); *Trump v. Clinton*, --- F. Supp.
22 3d ----, 2022 WL 16848187, at *5–8 (S.D. Fla. Nov. 10, 2022) (“The rule of law is

23 _____
24 count and verify votes, stating: “We the people deserve to know, on election night, the
25 of that.” Kari Lake (@KariLake), Twitter (Nov. 8, 2022, 10:40 p.m.),
26 <https://twitter.com/KariLake/status/1590217668849647616>, at 4:15–55. Given how long it
27 takes to hand count ballots—according to Plaintiffs’ own expert (Tr. 71:20–74:4), among
28 others—it is difficult, if not impossible, to square Plaintiff Lake’s election-night statements
with her position in this litigation that a full hand count should be required. At a minimum,
her statements are inconsistent with a “genuine belief” that hand counts are the only reliable
means of counting votes. While the Court finds this inconsistency troubling, it concludes
the Twitter post should not form any part of its decision, as the post is outside the record
of the case.

1 undermined by . . . efforts to advance a political narrative through lawsuits without factual
2 basis or any cognizable legal theory.”).

3 **B. 28 U.S.C. § 1927**

4 The Maricopa County Defendants also argue that sanctions against Plaintiffs’
5 counsel are independently warranted under 28 U.S.C. § 1927. (Mot. at 10–11.) They argue
6 that Plaintiffs’ counsel violated Section 1927 by making numerous false allegations and
7 misrepresentations, pursuing baseless claims, and moving for preliminary injunctive relief
8 even after counsel for Defendants alerted them that Plaintiffs’ claims were time-barred and
9 utterly lacking in support. (*Id.*) Defendants contend that the “inexplicable years-long delay
10 in seeking injunctive relief” is further evidence that Plaintiffs’ counsel have acted
11 improperly. (Mot. at 11.)

12 Plaintiffs argue that Defendants’ arguments fail because they do not show “that any
13 proceeding was ‘unreasonably’ or ‘vexatiously’ multiplied,” or provide evidence of
14 subjective bad faith. (Resp. at 16–17.) With respect to delay, Plaintiffs draw comparisons
15 to *Brown v. Board of Education*, 357 U.S. 483 (1954), and note that “[a] defendant’s
16 unconstitutional conduct is not immunized against legal challenge merely because a certain
17 amount of time passes before a plaintiff decides to challenge it.” (*Id.*)

18 The Court has already concluded that Plaintiffs’ claims are frivolous in that they are
19 “both baseless and made without a reasonable and competent inquiry.” *Townsend*, 929 F.2d
20 at 1362. It further agrees with Defendants that under the circumstances, it was objectively
21 unreasonable and vexatious for Plaintiffs’ counsel to initiate additional, time- and resource-
22 intensive preliminary injunction proceedings based on frivolous claims and to continue
23 making false and misleading representations about Arizona elections. The remaining
24 question under Section 1927 is whether Plaintiffs’ counsel acted recklessly or in bad faith.
25 *See Blixseth*, 796 F.3d at 1008. The Court concludes they did.

26 Plaintiffs’ counsel waited nearly seven weeks after filing this case to move for a
27 preliminary injunction, despite alleging imminent and irreparable injury in their original
28 Complaint. (*See Compl.* ¶¶ 156–66.) By the time of the MPI hearing on July 21, 2022, the

1 midterm election was fewer than four months away. As noted, the relief Plaintiffs requested
2 was remarkable and perhaps unprecedented. And as the Maricopa County Defendants note,
3 the timing of Plaintiffs’ MPI resulted in “wasting the time of election employees on the
4 eve of the August 2022 primary election and forcing the unnecessary expenditure of
5 taxpayer resources.” (Mot. at 11.) Further, Plaintiffs’ counsel filed the MPI soon after
6 counsel for the Maricopa County Defendants notified them as to the frivolousness of
7 Plaintiffs’ claims and the applicable bars to relief, including the *Purcell* doctrine.

8 Plaintiffs should have heeded the warning. In dismissing Plaintiffs’ claims, the
9 Court applied the *Purcell* doctrine, among others, and found that the relief Plaintiffs sought
10 “would not just be challenging for Arizona’s election officials to implement; it likely would
11 be impossible under the extant time constraints.” (Dismissal Order at 20.) Doctrinally and
12 practically, the *Purcell* doctrine encapsulates a central problem of Plaintiffs’ MPI:

13 [T]he principle . . . reflects a bedrock tenet of election law: When an election
14 is close at hand, the rules of the road must be clear and settled. Late judicial
15 tinkering with election laws can lead to disruption and to unanticipated and
16 unfair consequences for candidates, political parties, and voters, among
17 others. It is one thing for a State on its own to toy with its election laws close
to a State’s elections. But it is quite another thing for a federal court to swoop
in and re-do a State’s election laws in the period close to an election.

18 *Merrill v. Milligan*, 142 S. Ct. 879, 880–81 (2022) (Kavanaugh, J., concurring in grant of
19 applications for stays). Plaintiffs knew or reasonably should have known that the Court
20 could not and would not grant the wide-ranging, late-breaking relief they sought.¹¹ The
21 Court finds that Plaintiffs’ counsel acted at least recklessly in multiplying the proceedings.

22 **IV. SANCTIONS**

23 The Court concludes that sanctions are warranted under Rule 11 and 28 U.S.C.
24 § 1927. It finds that Plaintiffs made false, misleading, and unsupported factual assertions
25 in their FAC and MPI and that their claims for relief did not have an adequate factual or

26 ¹¹ Although Plaintiffs have filed a Notice of Appeal of the Court’s Dismissal Order, they
27 have yet to request emergency relief from the Ninth Circuit. *See* Docket, *Lake et al. v.*
28 *Hobbs et. al*, Ninth Circuit Case No. 22-16413. Of course, Plaintiffs and their counsel were
not obligated to seek such emergency relief, but it raises questions about the good faith
basis for their request for immediate relief filed in this Court based on allegedly imminent
and irreparable harm flowing from an election that has now already taken place.

1 legal basis grounded in a reasonable pre-filing inquiry, in violation of Rules 11(b)(2) and
2 (b)(3). The Court further finds that Plaintiffs’ counsel acted at least recklessly in
3 unreasonably and vexatiously multiplying the proceedings by seeking a preliminary
4 injunction based on Plaintiffs’ frivolous claims, in violation of Section 1927.

5 Two issues remain. First, the Court must identify the parties responsible for the
6 offending conduct. Rule 11 authorizes the Court to “to impose an appropriate sanction on
7 any attorney, law firm, or party that violated the rule or is responsible for the violation.”
8 Fed. R. Civ. P. 11(c)(1). The standard applicable to represented parties is more forgiving
9 than the attorney standard, as “represented parties may often be less able to investigate the
10 legal basis for a paper or pleading.” *Bus. Guides, Inc. v. Chromatic Commc’ns. Enters.*,
11 498 U.S. 533, 550 (1991). Moreover, represented parties cannot be sanctioned for
12 violations of Rule 11(b)(2) or Section 1927, both of which impose duties only on attorneys.

13 Here, while there are reasons to believe that Plaintiffs themselves contributed to the
14 violations of Rule 11(b)(3) in this case—including that they themselves apparently have
15 voted on paper ballots, contradicting allegations and representations in their pleadings
16 about Arizona’s use of paper ballots—there is not a sufficient record that compels the Court
17 to exercise its discretion to sanction Plaintiffs under that part of the rule. Thus, although
18 the Court does not find that Plaintiffs have acted appropriately in this matter—far from it—
19 the Court concludes that sanctions are warranted only against Plaintiffs’ counsel, who
20 signed and filed the offending papers. To sanction Plaintiffs’ counsel here is not to let
21 Plaintiffs off the hook. It is to penalize specific attorney conduct with the broader goal of
22 deterring similarly baseless filings initiated by anyone, whether an attorney or not.

23 Lastly, the Court must identify the appropriate sanction. Under Rule 11, the
24 “sanction imposed . . . must be limited to what suffices to deter repetition of the conduct
25 or comparable conduct by others similarly situated.” Fed. R. Civ. P. 11(c)(4). Where
26 sanctions are “imposed on motion and warranted for effective deterrence,” they may
27 include payment of reasonable attorneys’ fees. *Id.* Section 1927 likewise authorizes the
28 Court to order the payment of reasonable attorneys’ fees. 28 U.S.C. § 1927. Here, the Court

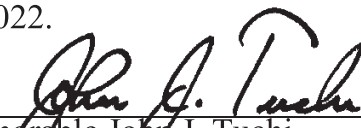
1 finds that payment of the Maricopa County Defendants' reasonable attorneys' fees is an
2 appropriate sanction for the conduct of Plaintiffs' counsel, which forced Defendants and
3 their counsel to spend time and resources defending this frivolous lawsuit rather than
4 preparing for the elections over which Plaintiffs' claims baselessly kicked up a cloud of
5 dust. Plaintiffs' counsel are therefore held jointly and severally liable for the Maricopa
6 County Defendants' attorneys' fees reasonably incurred in this case.

7 Imposing sanctions in this case is not to ignore the importance of putting in place
8 procedures to ensure that our elections are secure and reliable. It is to make clear that the
9 Court will not condone litigants ignoring the steps that Arizona has already taken toward
10 this end and furthering false narratives that baselessly undermine public trust at a time of
11 increasing disinformation about, and distrust in, the democratic process. It is to send a
12 message to those who might file similarly baseless suits in the future.

13 **IT IS THEREFORE ORDERED** granting the Maricopa County Defendants'
14 Rule 11 and 28 U.S.C. § 1927 Motion for Sanctions (Doc. 97).

15 **IT IS FURTHER ORDERED** that, within 14 days of entry of this Order, the
16 Maricopa County Defendants shall file a memorandum setting forth the attorneys' fees
17 they have reasonably incurred in this case from the time of the filing of Plaintiffs' first
18 Amended Complaint (Doc. 3) to the filing of this Order, along with supporting
19 documentation and in conformance with LRCiv 54.2. No later than 14 days thereafter,
20 Plaintiffs shall file any Response only as to the reasonableness of the requested award
21 under LRCiv 54.2(c)(3) and (f).

22 Dated this 1st day of December, 2022.

23 
24 _____
25 Honorable John J. Tuchi
26 United States District Judge
27
28

1 **PARKER DANIELS KIBORT**
Andrew Parker (028314)
2 888 Colwell Building
123 Third Street North
3 Minneapolis, Minnesota 55401
Telephone: (612) 355-4100
4 Facsimile: (612) 355-4101
parker@parkerdk.com
5 *Attorneys for Plaintiffs*

6 **UNITED STATES DISTRICT COURT**
7 **DISTRICT OF ARIZONA**

8 Kari Lake and Mark Finchem,
9 Plaintiffs,

No. 2:22-cv-00677-DMF

10 v.

AMENDED COMPLAINT

11
12 Kathleen Hobbs, as Arizona Secretary of
State; Bill Gates, Clint Hickman, Jack
13 Sellers, Thomas Galvin, and Steve
14 Gallardo, in their capacity as members of
the Maricopa County Board of Supervisors;
15 Rex Scott, Matt Heinz, Sharon Bronson,
Steve Christy, Adelita Grijalva, in their
16 capacity as members of the Pima County
Board of Supervisors,
17

(Jury Trial Demand)

18
19 1. This is a civil rights action for declaratory and injunctive relief to prohibit the use
20 of electronic voting machines in the State of Arizona in the upcoming 2022 Midterm Election,
21 slated to be held on November 8, 2022 (the “Midterm Election”), unless and until the electronic
22 voting system is made open to the public and subjected to scientific analysis by objective experts
23 to determine whether it is secure from manipulation or intrusion. The machine companies have
24 consistently refused to do this.

25 2. Plaintiffs have a constitutional and statutory right to have their ballots, and all
26 ballots cast together with theirs, counted accurately and transparently, so that only legal votes
determine the winners of each office contested in the Midterm Election. Electronic voting

1 machines cannot be deemed reliably secure and do not meet the constitutional and statutory
2 mandates to guarantee a free and fair election. The use of untested and unverified electronic voting
3 machines violates the rights of Plaintiffs and their fellow voters and office seekers, and it
4 undermines public confidence in the validity of election results. Just as the government cannot
5 insist on “trust me,” so too, private companies that perform governmental functions, such as vote
6 counting, cannot be trusted without verification

7 3. Defendants each have duties to ensure elections held with a “maximum degree of
8 correctness, impartiality, uniformity and efficiency on the procedures for early voting and voting,
9 and of producing, distributing, collecting, counting, tabulating and storing ballots.” A.R.S. § 16-
10 452 (A). Defendants have fallen short of those duties, and they will do so again unless this Court
11 intervenes.

12 4. For two decades, experts and policymakers from across the political spectrum have
13 raised glaring failures with electronic voting systems. Indeed, just three months ago, a computer
14 science expert in *Curling v. Raffensperger*, Case No. 1:17-cv-02989-AT (U.S. Dist. Ct., N.D.
15 Ga.), identified catastrophic failures in electronic voting machines used in sixteen states, including
16 Arizona. The expert testified that the failures include the ability to defeat all state safety
17 procedures. This caused the Cybersecurity and Infrastructure Security Agency (“CISA”) to enter
18 an appearance and urge the federal district court to not allow disclosure of the expert’s report
19 detailing these failures. The district court refused to allow disclosure of that expert report to date.
20 Secrecy destroys public confidence in our elections and election systems that result in secrecy
21 undermine our democratic process.

22 5. The problems with the electronic voting systems are not only technical, but
23 structural. To date, only three companies collectively provide voting machines and software for
24 90% of all eligible voters in the United States. Most of those machines are over a decade old,
25 have critical components manufactured overseas in countries, some of which are hostile to the
26 United States, and use software that is woefully outdated and vulnerable to catastrophic

1 cyberattacks. Indeed, countries like France have banned the use of electronic voting machines
2 due to lack of security and related vulnerabilities.

3 6. Given the limitations and flaws of existing technology, electronic voting machines
4 cannot legally be used to administer elections today and for the foreseeable future, unless and until
5 their current electronic voting system is objectively validated.

6 7. Through this Action, Plaintiffs seek an Order that Defendants collect and count
7 votes through a constitutionally acceptable process, which relies on tried and true precepts that
8 mandates integrity and transparency. This includes votes cast by hand on verifiable paper ballots
9 that maintains voter anonymity; votes counted by human beings, not by machines; and votes
10 counted with transparency, and in a fashion observable to the public.

11 8. It is important to note that this Complaint is not an attempt to undo the past. Most
12 specifically, it is not about undoing the 2020 presidential election. It is only about the future –
13 about upcoming elections that will employ voting machines designed and run by private
14 companies, performing a crucial governmental function, that refuse to disclose their software and
15 system components and subject them to neutral expert evaluation. It raises the profound
16 constitutional issue: can government avoid its obligation of democratic transparency and
17 accountability by delegating a critical governmental function to private companies?

18 **I. INTRODUCTION**

19 9. The Arizona Constitution provides that “[a]ll elections shall be free and equal.”
20 Ariz. Const. art. 2 § 21. Defendant Hobbs, as Arizona Secretary of State and the chief election
21 officer in Arizona, has enabled a process fundamentally at odds with this requirement..

22 10. Defendant Hobbs violated state and federal law in several respects, including her
23 failure to:

- 24 • Achieve and maintain the maximum degree of correctness, impartiality, uniformity
25 in elections.
26 • Ensure that all votes are counted safely, efficiently, and accurately.

- 1
- 2 • Ensure that all software code, firmware code, and hard-coded instructions on any
- 3 hardware component used, temporarily or installed in the voting systems, precludes
- 4 fraud or any unlawful act.
- 5 • Revoke the certification of electronic voting systems used in elections in Arizona.
- 6 • Demand access to the electronic voting system so that it can be examined by
- 7 objective experts.

8 11. Defendant Hobbs intends to commit these same violations up to and during the

9 Midterm Election.

10 12. Defendants Gates, Hickman, Sellers, Galvin, and Gallardo, as Members of the

11 Maricopa County Board of Supervisors, have caused the use of election systems and equipment

12 in Maricopa County that are rife with potentially glaring cybersecurity vulnerabilities, including

- 13 • Operating systems lacking necessary updates;
- 14 • Antivirus software lacking necessary updates;
- 15 • Open ports on the election management server, allowing for possible remote access;
- 16 • Shared user accounts and common passwords;
- 17 • Anomalous, anonymous logins to the election management server;
- 18 • Unexplained creation, modification, and deletion of election files;
- 19 • Lost security log data;
- 20 • The presence of stored data from outside of Maricopa County;
- 21 • Unmonitored network communications;
- 22 • Unauthorized user internet or cellular access through election servers and devices.
- 23 • Secret content not subject to objective and public analysis.

24 13. Pima County uses election equipment and systems that are in substance and defect

25 the same as the equipment and systems used in Maricopa County. Defendants Scott, Heinz,

26 Bronson, Christy, and Grijalvaas, as Members of the Pima County Board of Supervisors, have

1 caused the use of election systems and equipment in Pima County that are rife with the same
2 glaring potential cybersecurity vulnerabilities present in the Maricopa County equipment.

3 14. Every county in Arizona intends to tabulate votes cast in the Midterm Elections
4 through optical scanners, the vast majority of which are manufactured by Election Systems &
5 Software (“ES&S”) or Dominion Voting Systems (“Dominion”).

6 15. After votes are tabulated at the county level using these machines through these
7 companies’ proprietary election management systems, the vote tallies will be uploaded over the
8 internet to an election reporting system.

9 16. Some voters in Arizona will rely on electronic voting systems to cast their votes as
10 well as tabulate them. Voters who may have hearing or visual impairments may cast their votes
11 with the aid of electronic ballot marking devices manufactured primarily by ES&S or Dominion.
12 These voters’ electoral choices are even more vulnerable to attack and manipulation, as ballot
13 marking devices pose significant security risks on their own.

14 17. Defendant Hobbs, through the website of the Office of the Arizona Secretary of
15 State, has represented that counties throughout Arizona will rely on electronic voting systems in
16 the Midterm Election.

17 18. Defendant Hobbs on or about November 5, 2019, certified the Dominion
18 Democracy Suite 5.5b voting system for use in elections held in Arizona. This voting system, as
19 well as the component parts identified above, will be used in the Midterm Election.

20 19. Defendant Hobbs after July 22, 2020, certified the ES&S ElectionWare 6.0.40
21 voting system, as well as its component parts, for use in elections held in Arizona. This voting
22 system, as well as the component parts identified above, will be used in the Midterm Election.¹

23 20. Defendant Hobbs’s certification of the Dominion Democracy Suite 5.5b voting
24 system, as well as its component parts, was improper, absent objective evaluation.

25
26

¹ See <https://azsos.gov/elections/voting-election/voting-equipment>.

1 21. Defendant Hobbs’s certification of the ES&S ElectionWare 6.0.40 voting system,
2 as well as its component parts, was improper.

3 22. Defendant Hobbs has the authority to revoke the certification of every voting
4 system, including all component parts thereto, certified by the State of Arizona. Defendant Hobbs
5 has improperly failed to exercise that authority.

6 23. All optical scanners and ballot marking devices certified by Arizona, as well as the
7 software on which they rely, have been wrongly certified for use in Arizona. These systems are
8 potentially unsecure, lack adequate audit capacity, fail to meet minimum statutory requirements,
9 and deprive voters of the right to have their votes counted and reported in an accurate, auditable,
10 legal, and transparent process. Using them in the upcoming elections, without objective validation,
11 violates the voting rights of every Arizonan.

12 24. All electronic voting machines and election management systems, including those
13 slated to be used in Arizona in the Midterm Election, can be manipulated through internal or
14 external intrusion to alter votes and vote tallies.

15 25. Specific vulnerabilities in the electronic voting machines used by Maricopa County
16 have been explicitly identified and publicized in analyses by cybersecurity experts, even absent
17 access to the systems.

18 26. Substantially similar vulnerabilities in electronic voting machines in general have
19 been identified and publicized in analyses presented to various congressional committees. All
20 electronic voting machines can be connected to the internet or cellular networks, directly or
21 indirectly, at various steps in the voting, counting, tabulating, and/or reporting process.

22 27. Voting machines and systems used in Arizona contain electronic components
23 manufactured or assembled in foreign nations which have attempted to manipulate the results of
24 U.S. elections.

25

26

1 28. Electronic voting machines and software manufactured by industry leaders,
2 specifically including Dominion and ES&S, are vulnerable to cyberattacks before, during, and
3 after an election in a manner that could alter election outcomes.

4 29. These systems can be connected to the internet or cellular networks, which provides
5 an access point for unauthorized manipulation of their software and data. They often rely on
6 outdated versions of Windows, which lack necessary security updates. Both of these common
7 shortcomings leave the systems vulnerable to generalized, widespread-effect attacks.

8 30. Since 2000, alleged, attempted, and actual illegal manipulation of votes through
9 electronic voting machines has apparently occurred on multiple occasions.

10 31. Expert testimony demonstrates that all safety measures intended to secure electronic
11 voting machines against manipulation of votes, such as risk limiting audits and logic and accuracy
12 tests, can be defeated.

13 32. Other countries, including France and Taiwan, have completely or largely banned
14 or limited the use of electronic voting machines due to the security risks they present.

15 33. Arizona's electronic election infrastructure is potentially susceptible to malicious
16 manipulation that can cause incorrect counting of votes. Despite a nationwide bipartisan
17 consensus on this risk, election officials in Arizona continue to administer elections dependent
18 upon unreliable, insecure electronic voting systems. These officials, including Defendants in
19 Maricopa County, refuse to take necessary action to address known and currently unknown
20 election security vulnerabilities, and in some cases have obstructed court authorized inspections
21 of their electronic voting systems.

22 34. Plaintiffs seek the intervention of this Court because the Secretary of State and
23 county officials throughout the State have failed to take constitutionally necessary measures to
24 protect voters' rights to a secure and accurately counted election process. The State of Arizona
25 and its officials bear a legal, constitutional, and ethical obligation to secure the State's electoral
26 system, but they lack the will to do so.

1 **I. PARTIES**

2 35. Plaintiff Kari Lake is a candidate for Governor of Arizona, an office she seeks in
3 the Midterm Election.

4 36. Plaintiff Kari Lake is also a resident of the State of Arizona, registered to vote in
5 Maricopa County, who intends to vote in Arizona in the Midterm Election.

6 37. Plaintiff Mark Finchem is a sitting member of the Arizona House of Representatives
7 and a candidate for Secretary of State of Arizona, an office he seeks in the Midterm Election.

8 38. Plaintiff Mark Finchem is also a resident of the State of Arizona, registered to vote
9 in Pima County, who intends to vote in Arizona in the Midterm Election.

10 39. Plaintiff Lake has standing to bring this action as an intended voter in the Midterm
11 Election and as a “qualified elector” under A.R.S. § 16-121. As a candidate for Governor of
12 Arizona Plaintiff Lake further has standing as an aggrieved person to bring this action.

13 40. Plaintiff Finchem, in his capacity as a member of the Arizona House of
14 Representatives charged with upholding the Constitution of the United States, has standing to
15 bring this action.

16 41. Plaintiff Finchem has standing to bring this action as an intended voter in the
17 Midterm Election and as a “qualified elector” under A.R.S. § 16-121. As a candidate for Secretary
18 of State of Arizona Plaintiff Finchem further has standing as an aggrieved person to bring this
19 action.

20 42. Defendant Hobbs is, through this Complaint, sued for prospective declaratory and
21 injunctive relief in her official capacity as the Secretary of State of Arizona, together with any
22 successor in office automatically substituted for Defendant Hobbs by operation of Fed. R. Civ. P.
23 25(d).

24 43. In her official capacity, Defendant Hobbs is the chief election officer for the State
25 of Arizona. Defendant Hobbs is responsible for the orderly and accurate administration of public
26 election processes in the state of Arizona. This responsibility includes a statutory duty to ensure

1 that “satisfactorily tested” voting systems are used to administer public elections, A.R.S. § 16-
2 441, and to conduct any reexaminations of previously adopted voting systems, upon request or at
3 Defendant Hobbs’s own discretion.

4 44. Defendant Hobbs is further required by law to determine the voting equipment that
5 is to be used to cast and count the votes in all county, state, and federal elections in Arizona, and
6 to prescribe an official instructions and procedures manual before each such election. A.R.S. §§
7 16-446, 16-452.

8 45. Defendants Bill Gates, Clint Hickman, Jack Sellers, Thomas Galvin, and Steve
9 Gallardo (collectively “Maricopa Defendants”) are sued for prospective declaratory and injunctive
10 relief in their official capacities as members of the Maricopa County Board of Supervisors
11 (“Maricopa Board”).

12 46. Defendants Scott, Heinz, Bronson, Christy, and Grijalva (collectively “Pima
13 Defendants”) are sued for prospective declaratory and injunctive relief in their official capacities
14 as members of the Pima County Board of Supervisors (“Pima Board”).

15 47. Under A.R.S. § 16-452 (A), the Maricopa Board and the Pima Board are vested with
16 the authority to:

- 17 • “[e]stablish, abolish and change election precincts, appoint inspectors and judges of
18 elections, canvass election returns, declare the result and issue certificates
19 thereof...”;
- 20 • “[a]dopt provisions necessary to preserve the health of the county, and provide for
21 the expenses thereof”;
- 22 • “[m]ake and enforce necessary rules and regulations for the government of its body,
23 the preservation of order and the transaction of business.”

1 **II. JURISDICTION AND VENUE**

2 48. Plaintiffs bring this action under 42 U.S.C. § 1983 and the cause of action
3 recognized in *Ex parte Young*, 209 U.S. 123 (1908), and its progeny to challenge government
4 officers’ “ongoing violation of federal law and [to] seek[] prospective relief” under the equity
5 jurisdiction conferred on federal district courts by the Judiciary Act of 1789.

6 49. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1343
7 because this action seeks to protect civil rights under the Fourteenth Amendment to the United
8 States Constitution.

9 50. This Court has supplemental jurisdiction over Plaintiffs’ claims under 28 U.S.C. §
10 1367.

11 51. This Court has authority to grant declaratory relief based on 28 U.S.C. §§ 2201 &
12 2202, and Rule 57 of the Federal Rules of Civil Procedure.

13 52. This Court has jurisdiction to grant injunctive relief based on 28 U.S.C. § 1343(a)(3)
14 and authority to do so under Federal Rule of Civil Procedure 65.

15 53. This Court has jurisdiction to award nominal and compensatory damages under 28
16 U.S.C. § 1343(a)(4).

17 54. This Court has authority to award reasonable attorneys’ fees and costs. 28 U.S.C. §
18 1920 and 42 U.S.C. § 1988(b).

19 55. Venue is proper in this Court under 28 U.S.C. § 1391(b) because a substantial part
20 of the events or omissions giving rise to Plaintiff’s claims occurred in this District.

21 56. This Court has personal jurisdiction over all Defendants because all defendants
22 reside and are domiciled in the State of Arizona. Requiring Defendants to litigate these claims in
23 the United States District Court for the District of Arizona does not offend traditional notions of
24 fair play and substantial justice and is permitted by the Due Process Clause of the United States
25 Constitution.

26

III. FACTUAL ALLEGATIONS

A. Background

57. Arizona intends to rely on electronic voting systems to record some votes and to tabulate *all* votes cast in the State of Arizona in the 2022 Midterm Election, without disclosing the systems and subjecting them to neutral, expert analysis.²

58. Prior to 2002, most states, including Arizona, conducted their elections overwhelmingly using relatively secure, reliable, and auditable paper-based systems.

59. After the recount of the 2000 presidential election in Florida and the ensuing *Bush v. Gore* decision, Congress passed the Help America Vote Act in 2002.³ In so doing, Congress opened the proverbial spigot. Billions of federal dollars were spent to move states, including Arizona, from paper-based voting systems to electronic, computer-based systems.

60. Since 2002, elections throughout the United States have increasingly and largely been conducted using a handful of computer-based election management systems. These systems are created, maintained, and administered by a small number of companies having little to no transparency to the public, producing results that are far more difficult to audit than paper-based systems, and lack any meaningful federal standards or security requirements beyond what individual states may choose to certify. Leaders of both major parties have expressed concern about this lack of transparency, analysis and accountability.

61. As of 2019, Dominion, ES&S, and one other company (Hart InterCivic) supplied more than ninety percent of the nationwide “voting machine market.”⁴ Dominion and ES&S control even more than that share of the market in Arizona. All three of these providers’ electronic

²<https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2022/state/4>

³ 52 U.S.C. § 20901 *et seq.*

⁴ Pam Fessler & Johnny Kauffman, *Trips to Vegas and Chocolate-Covered Pretzels: Election Vendors Come Under Scrutiny*, NPR (May 2, 2019) (<https://www.npr.org/2019/05/02/718270183/trips-to-vegas-and-chocolate-covered-pretzels-election-vendors-come-under-scruti>).

1 voting machines can be hacked or compromised with malware, as has been demonstrated by
2 recognized computer science experts, including experts from the University of Michigan,
3 Princeton University, Georgetown University, and other institutions and presented to various
4 congressional committees. All can be, and at various steps in the voting, counting, tabulating,
5 and/or reporting process are designed to be, connected to the internet or cellular networks, directly
6 or indirectly.

7 62. This small cadre of companies supplies the hardware and software for the electronic
8 voting machines, in some cases manages the voter registration rolls, maintains the voter records,
9 partially manages the elections, programs the vote counting, and reports the election results.

10 63. Jurisdictions throughout the nation, including Arizona, have functionally
11 outsourced all election operations to these private companies. In the upcoming Midterm Election,
12 over three thousand counties across the United States will have delegated the governmental
13 responsibility for programming and administering elections to private contractors.

14 64. This includes all counties in Arizona, most of which have contracted with Dominion
15 or ES&S to provide machines, software, and services for the Midterm Election. For example, in
16 Defendant Maricopa County, officials do not possess credentials necessary to validate tabulator
17 configurations and independently validate the voting system prior to an election. Dominion
18 maintains those credentials.

19 65. By its own account, Dominion provides an “End-To-End Election Management
20 System” that “[d]rives the entire election project through a single comprehensive database.”⁵ Its
21 tools “build the election project,” and its technology provides “solutions” for “voting &
22 tabulation,” and “tallying & reporting,” and “auditing the election.” The products sold by
23 Dominion include ballot marking machines, tabulation machines, and central tabulation machines,
24 among others.

25
26

⁵ DEMOCRACY SUITE® ELECTION MANAGEMENT SYSTEM,
<https://www.dominionvoting.com/democracy-suite-ems/> (last visited Apr. 22, 2022).

1 66. Dominion, in its normal course of business, including the Midterm Election in
2 Arizona, manufactures, distributes, and maintains voting hardware and software. Dominion also
3 executes software updates, fixes, and patches for its voting machines and election management
4 systems.

5 67. After votes are tabulated at the county level using Dominion’s electronic election
6 management system in the Midterm Election, the vote tallies will be uploaded over the internet to
7 an election reporting system.

8 68. Dominion’s machines and systems range from the “election event designer”—
9 software that creates the ballots voters will mark while voting, as well as programing the tabulators
10 of those votes—to the devices on which voters mark their votes (“ballot marking devices,” or
11 “BMDs”), to the machines that tabulate the votes at the precinct level, to the machines that receive
12 and tabulate the various precinct results (“centralized tabulation”), to the systems and options for
13 transmitting those results from the BMD to the precinct tabulator to the central tabulator to,
14 ultimately, the official government authority responsible for certifying the election results. In the
15 Midterm Election, many Arizonans will cast their votes on Dominion BMDs, while nearly *all*
16 Arizonans will have their votes tabulated with Dominion machines.

17 69. Dominion controls the administration and conduct of the elections in those
18 jurisdictions where its systems are deployed, including Arizona. Any vulnerabilities or
19 weaknesses in Dominion’s systems, at the very least, call into question the integrity and reliability
20 of all election results coming from those jurisdictions. Dominion has refused to disclose its
21 software and other parts of its electronic voting system in order to subject it to neutral expert
22 evaluation.

23 70. As an example, following the 2020 election an audit of election processes and
24 results in Maricopa County, Arizona was ordered. It was concluded that:

- 25 • “The official result totals do not match the equivalent totals from the Final Voted
26 File (VM55). These discrepancies are significant with a total ballot delta of 11,592

1 between the official canvass and the VM55 file when considering both the counted
2 and uncounted ballots.”;

- 3 • “...a large number of files on the Election Management System (EMS) Server and
4 HiPro Scanner machines were deleted including ballot images, election related
5 databases, result files, and log files. These files would have aided in our review and
6 analysis of the election systems as part of the audit. The deletion of these files
7 significantly slowed down much of the analysis of these machines. Neither of the
8 ‘auditors’ retained by Maricopa County identified this finding in their reports.”; and
- 9 • “Despite the presence of at least one poll worker laptop at each voting center, the
10 auditors did not receive laptops or forensic copies of their hard drives. It is
11 unknown, due to the lack of this production, whether there was unauthorized access,
12 malware present or internet access to these systems.”

13 **B. Decades of Evidence Prove Electronic Voting Systems Do Not Provide a**
14 **Secure, Transparent, or Reliable Vote**

15 71. Over the last two decades the United States has transitioned from a safe, secure,
16 auditable paper-based system to an inherently vulnerable, network-exposed electronic equipment-
17 based system. The transition to increased reliance on electronic systems and computer technology
18 has created unjustified new risks of hacking, election tampering, and electronic voting fraud.

19 72. With each passing election the unreliability of electronic voting machines has
20 become more apparent. In light of this experience, the vote tallies reported by electronic voting
21 machines cannot, without objective evaluation, be trusted to accurately show which candidates
22 actually received the most votes.

23 73. Credible allegations of electronic voting machine “glitches” that materially
24 impacted specific races began to emerge in 2002. *Black Box Voting*, the seminal publication
25 documenting early pitfalls of electronic voting systems, chronicles failures that include:
26

- 1 • “In the Alabama 2002 general election, machines made by Election Systems
2 and Software (ES&S) flipped the governor’s race. Six thousand three
3 hundred Baldwin County electronic votes mysteriously disappeared after the
4 polls had closed and everyone had gone home. Democrat Don Siegelman’s
5 victory was handed to Republican Bob Riley, and the recount Siegelman
6 requested was denied. Six months after the election, the vendor shrugged.
7 ‘Something happened. I don’t have enough intelligence to say exactly what,’
8 said Mark Kelley of ES&S.”
- 9 • “In the 2002 general election, a computer miscount overturned the House
10 District 11 result in Wayne County, North Carolina. Incorrect programming
11 caused machines to skip several thousand partyline votes, both Republican
12 and Democratic. Fixing the error turned up 5,500 more votes and reversed
13 the election for state representative.”
- 14 • “Voting machines failed to tally ‘yes’ votes on the 2002 school bond issue in
15 Gretna, Nebraska. This error gave the false impression that the measure had
16 failed miserably, but it actually passed by a 2 to 1 margin. Responsibility for
17 the errors was attributed to ES&S, the Omaha company that had provided the
18 ballots and the machines.”
- 19 • “In the November 2002 general election in Scurry County, Texas, poll
20 workers got suspicious about a landslide victory for two Republican
21 commissioner candidates. Told that a ‘bad chip’ was to blame, they had a
22 new computer chip flown in and also counted the votes by hand — and found
23 out that Democrats actually had won by wide margins, overturning the
24 election.”⁶

⁶ Available at <https://blackboxvoting.org/black-box-voting-book/>.

1 74. By 2004, explicit evidence that electronic voting machines were susceptible to
2 intentional manipulation, and that malicious actors sought to exploit this vulnerability, became
3 public. In that year, cyber expert Clint Curtis testified under oath before the House Judiciary
4 Committee that he had previously been hired to create a program that would change the results of
5 an election without leaving any trace of the change. He claimed he wrote this program with ease.
6 Mr. Curtis' testimony can be watched here: <https://www.youtube.com/watch?v=JEzY2tnwExs>.

7 75. During the next election cycle, in 2006, a team of computer scientists at Princeton
8 University analyzed the Diebold AccuVote-TS voting machine, then one of the most widely-
9 deployed electronic voting platforms in the United States. They found, "Malicious software
10 running on a single voting machine can steal votes with little risk of detection. The malicious
11 software can modify all of the records, audit logs, and counters kept by the voting machine, so
12 that even careful forensic examination of these records will find nothing amiss. . . . Anyone who
13 has physical access to a voting machine, or to a memory card that will later be inserted into a
14 machine, can install said malicious software using a simple method that takes as little as one
15 minute. . . . AccuVote-TS machines are susceptible to voting machine viruses – computer viruses
16 that can spread malicious software automatically and invisibly from machine to machine during
17 normal pre- and post-election activity." The Princeton team prepared a video demonstration
18 showing how malware could flip votes. In the video, mock election votes were cast in favor of
19 George Washington by a 4 to 1 margin, but the paper print-out that reported the results showed
20 Benedict Arnold prevailing by a margin of 3 to 2. Malicious vote-stealing malware was the sole
21 reason for reallocation of votes. The malware deleted itself after the election, leaving no evidence
22 that the voting machine was ever hijacked or any votes stolen.

23 76. In 2009 Diebold sold (at a loss) "Premier," its electronic voting systems business
24 unit, which by then was known for its technical problems and unreliable security and accuracy.
25 The Premier intellectual property passed (from ES&S) to Dominion in May 2010. That
26 intellectual property included the GEMS election management system software. Dominion

1 quickly incorporated GEMS into its own products and by 2011 was selling election equipment
2 that had updated GEMS software at its heart. But GEMS was notorious for being, according to
3 Harper’s Magazine, “a vote rigger’s dream” that “could be hacked, remotely or on-site, using any
4 off-the-shelf version of Microsoft Access, and password protection was missing for supervisor
5 function.” Lack of encryption on its audit logs “allowed any trace of vote rigging to be wiped
6 from the record.” Computer scientists from Johns Hopkins University and Rice University found
7 GEMS “far below even the most minimal security standards applicable in other contexts” and
8 “unsuitable for use in a general election.”

9 77. In 2015 the Brennan Center for Justice issued a report listing two and a half-pages
10 of instances of issues with voting machines, including a 2014 investigation which found “voters
11 in Virginia Beach observed that when they selected one candidate, the machine would register
12 their selection for a different candidate.”⁷ The investigation also found that the Advanced Voting
13 Solutions WINVote machine, which is Wi-Fi-enabled, “had serious security vulnerabilities”
14 because wireless cards on the system could allow “an external party to access the [machine] and
15 modify the data [on the machine] without notice from a nearby location,” and “an attacker could
16 join the wireless ad-hoc network, record voting data or inject malicious [data.]”

17 78. In 2016, following in the footsteps of the Johns Hopkins, Rice, and 2006 Princeton
18 teams, Princeton Professor of Computer Science Andrew Appel told an interviewer how he had
19 purchased a voting machine for \$82 on the internet – the Sequoia AVC Advantage, still set to be
20 used in the 2016 election in a number of states – and replaced the machine’s ROM chips in mere
21 minutes using little more than a screwdriver, thereby “throw[ing] off the machine’s results, subtly
22 altering the tally of votes, never to betray a hint to the voter.”⁸

23 _____
24 ⁷ Lawrence Norden and Christopher Famighetti, *America’s Voting Machines at Risk*, Brennan
25 Center for Justice, p.13 (Sep. 15, 2014) (available at [https://www.brennancenter.org/our-
work/research-reports/americas-voting-machines-risk](https://www.brennancenter.org/our-work/research-reports/americas-voting-machines-risk)).

26 ⁸ Ben Wofford, *How to Hack an Election in 7 Minutes*, Politico (Aug. 5, 2016)
([https://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-
election-in-seven-minutes-214144/](https://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144/)).



79. During that 2016 election cycle evidence emerged of foreign state actors seeking to affect U.S. voting. “Russian agents probed voting systems in all 50 states, and successfully breached the voter registration systems of Arizona and Illinois.”⁹ The Robert Mueller report and an indictment of twelve Russian agents later confirmed that Russian hackers had targeted vendors that provide election software, and Russian intelligence officers “targeted employees of [REDACTED], a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network.”¹⁰

80. After these revelations about the 2016 election, Jake Braun, a former security advisor for the Obama administration and organizer of the DEFCON Hacking Conference was asked in 2017, “Do you believe that right now, we are in a position where the 2020 election will be hacked?” He answered, “Oh, without question. I mean the 2020 election will be hacked no matter what we do.”

⁹ Jordan Wilkie, ‘They think they are above the law’: the firms that own America’s voting system, *The Guardian* (Apr. 23, 2019) (<https://www.theguardian.com/us-news/2019/apr/22/us-voting-machine-private-companies-voter-registration>).

¹⁰ Robert S. Mueller, III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, vol. 1, p. 51 (Mar. 2019). (<https://www.justice.gov/archives/sco/file/1373816/download>).

1 81. Following a 2017 runoff election in a Georgia congressional race, an advocacy
2 organization and individual voters filed suit in federal district court seeking to set aside the results.
3 They alleged the election “took place in an environment in which sophisticated hackers – whether
4 Russian or otherwise – had the capability and intent to manipulate elections in the United States”
5 and had “easy access” to do so.

6 82. The Georgia plaintiffs supported their allegations with expert testimony from Logan
7 Lamb, who testified that he freely accessed official Georgia state election files hosted on an
8 “elections.kennesaw.edu” server, including voter histories and personal information of all Georgia
9 voters; tabulation and memory card programming databases for past and future elections;
10 instructions and passwords for voting equipment administration; and executable programs
11 controlling essential election resources. Lamb stated that these sensitive files had been publicly
12 exposed for so long that Google had cached (i.e., saved digital backup copies of) and published
13 the pages containing many of them. Lamb said the publicly accessible files created and maintained
14 on this server were used to program virtually all other voting and tabulation equipment used in
15 Georgia’s elections.

16 83. Another piece of expert evidence in the Georgia litigation is a declaration from Harri
17 Hursti dated August 24, 2020 in which Hursti concludes that “the voting system is being operated
18 in Fulton County in a manner that escalates the security risk to an extreme level.” Hursti based
19 this conclusion in part on his observations that optical scanners would inexplicably reject ballots;
20 that the optical scanners would experience lengthy and unexplained scanning delays; that the
21 vendor, Dominion, failed to ensure a trained technician was on-site to address problems with its
22 equipment; that Dominion employees interfered with Hursti’s efforts to observe the upload of
23 memory devices; that Dominion refused to cooperate with county personnel; and that computers
24 running Dominion software were vulnerable due to inadequate “hardening” against a security
25 attack.¹¹

26
¹¹ *Curling v. Raffensperger*, Case No. 1:17-cv-02989-AT (U.S. Dist. Ct., N.D. Ga.), ECF Doc.

1 84. The Georgia plaintiffs asked the court to enter a preliminary injunction barring
2 Georgia in the 2020 general election from using certain Dominion electronic voting machines. On
3 October 11, 2020, the federal court issued an order finding substantial evidence that the system
4 was plagued by security risks and the potential for votes to be improperly rejected or misallocated.
5 It wrote, “The Plaintiffs’ national cybersecurity experts convincingly present evidence that this is
6 not a question of ‘might this actually ever happen?’ – but ‘when it will happen.’”

7 85. Concerns in Georgia proved to be well-founded. After scanned ballot images were
8 designated as “public records” under Georgia Senate Bill 202, a report made public by VoterGA
9 revealed, among other things, that 17,724 votes in Fulton County were somehow counted and
10 certified through tabulation machines, despite having no corresponding ballot images. The report
11 further concluded that 132,284 mail-in ballot images do not have a .sha signature file, meaning
12 these ballots cannot be authenticated.

13 86. In 2019 a group of election security experts found “nearly three dozen backend
14 election systems in 10 states connected to the internet over the last year,” including in “critical
15 swing states” Wisconsin, Michigan, and Florida. Some of the jurisdictions “were not aware that
16 their systems were online” and were “publicly saying that their systems were never connected to
17 the internet because they didn’t know differently.”¹² The Associated Press reported that the vast
18 majority of 10,000 election jurisdictions nationwide were still using Windows 7 or older operating
19 systems to create ballots, program voting machines, tally votes, and report counts, which was a
20 problem because “Windows 7 reaches its ‘end of life’ on Jan. 14 [2020], meaning Microsoft stops
21 providing technical support and producing “patches” to fix software vulnerabilities, which hackers
22 can exploit.”¹³

23 _____
24 809-3.

25 ¹² Kim Zetter, *Critical U.S. Election Systems Have Been Left Exposed Online Despite Official*
26 *Denials*, Vice (Aug. 8, 2019) (<https://www.vice.com/en/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials>).

¹³ Tami Abdollah, *New election systems use vulnerable software*, Associated Press (July 13, 2019) (<https://apnews.com/article/operating-systems-ap-top-news-voting-voting-machines->

1 87. Prior to 2020, ES&S had represented to its customers and potential customers that
2 its DS200 voting system was “fully certified and compliant with EAC guidelines” even if used
3 with a modem—a critical access point by which unauthorized access can be made. In a letter
4 dated March 20, 2020, the U.S. Election Assistance Commission (EAC) issued a letter to ES&S
5 stating that ES&S had misrepresented that its voting machines with modems were EAC compliant.
6 The EAC ordered ES&S to take corrective actions, including to:

- 7 • Revise ES&S’s marketing material to properly represent voting systems that have
8 been certified by the EAC.
- 9 • Provide the EAC with a plan to removal all misrepresented marketing material from
10 circulation.
- 11 • Notify ES&S’s customers and potential customers that previous information was
12 inaccurate.
- 13 • Provide customers and potential customers with corrected information.

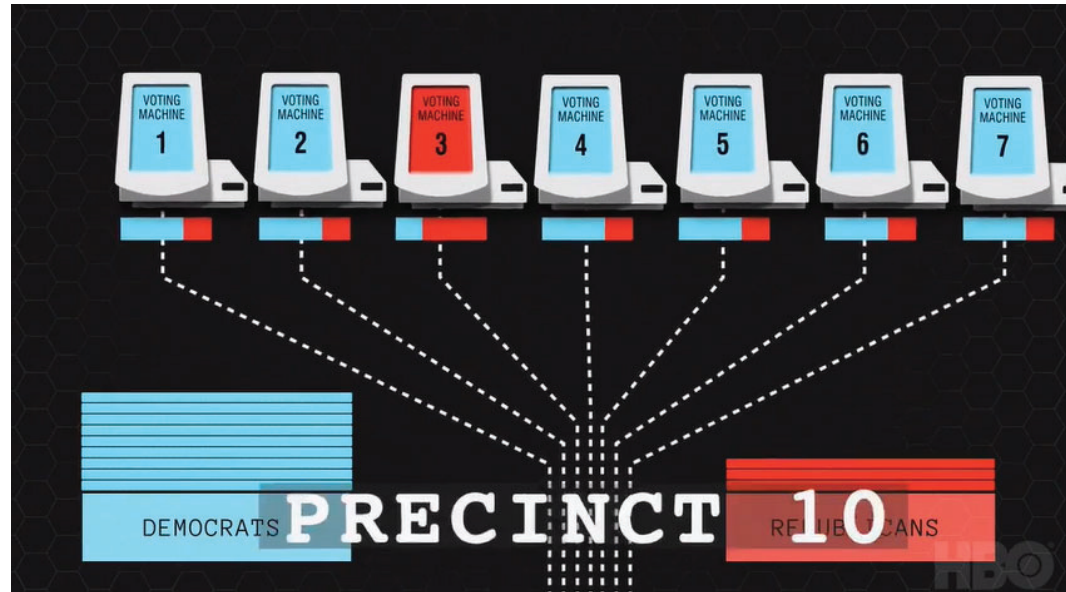
14 88. This is not the first time that ES&S has been caught in a lie about the voting
15 machines it sells. In 2018, Vice reported that ES&S falsely denied selling voting machines with
16 remote access software, a fact ES&S later admitted was true in a letter to Senator Ron Wyden (D.
17 Or.).¹⁴

18 89. In March 2020, the documentary *Kill Chain: The Cyber War on America’s Elections*
19 detailed the vulnerability of electronic voting machines. In the film, Hursti showed that he hacked
20 digital election equipment to change votes back in 2005, and said the same Dominion machine
21 that he hacked in 2005 was slated for use in 20 states for the 2020 election. *Kill Chain* also
22 included facts about a Georgia election in which one machine out of seven in a precinct registered
23 a heavy majority of Republican votes, while every other machine in the precinct registered a heavy
24

25 [pennsylvania-e5e070c31f3c497fa9e6875f426ccdel\).](https://www.vice.com/en/article/mb4ezy/top-voting-machine-vendor-admits-it-installed-remote-access-software-on-systems-sold-to-states)

26 ¹⁴ Kim Zetter, *Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States*, Vice (July 17, 2018) (<https://www.vice.com/en/article/mb4ezy/top-voting-machine-vendor-admits-it-installed-remote-access-software-on-systems-sold-to-states>).

majority of Democratic votes. Dr. Kellie Ottoboni, Department of Statistics, UC Berkeley, stated the likelihood of this happening by chance was less than one in a million.¹⁵



C. Electronic Voting Systems Manufacturers Source and Assemble Their Components in Hostile Nations

90. Electronic voting machines are also vulnerable to malicious manipulation through illicit software installed on their component parts during the manufacturing process. The Congressional Task Force on Election Security’s Final Report in January 2018 stated, “many jurisdictions are using voting machines that are highly vulnerable to an outside attack,” in part because “many machines have foreign-made internal parts.” Therefore, “[A] hacker’s point-of-entry into an entire make or model of voting machine could happen well before that voting machine rolls off the production line.”¹⁶

91. Computer server security breaches as a result of hardware manufactured in China have been discovered by the U.S. Department of Defense (2010), Intel Corp. (2014), an FBI

¹⁵ Screenshot from <https://www.facebook.com/KillChainDoc/videos/2715244992032273/>.

¹⁶ CONGRESSIONAL TASK FORCE ON ELECTION SECURITY, FINAL REPORT at 25 (2018) (<https://homeland.house.gov/imo/media/doc/TFESReport.pdf>).

1 investigation that affected multiple companies (2015), and a government contractor providing
2 intelligence services (2018).¹⁷

3 92. Leading electronic voting machine manufacturers source many parts from China,
4 Taiwan, and the Philippines.¹⁸

5 **D. State and Federal Lawmakers from Both Parties Have Long Been Aware of**
6 **the Problems with Electronic Voting Systems**

7 93. As the years passed and the evidence mounted, lawmakers and officials throughout
8 the nation have realized these problems with electronic voting machines cannot be ignored.

9 94. The Congressional Task Force on Election Security issued a Final Report in January
10 2018 that identified the vulnerability of U.S. elections to foreign interference:¹⁹ “According to
11 DHS, Russian agents targeted election systems in at least 21 states, stealing personal voter records
12 and positioning themselves to carry out future attacks. . . media also reported that the Russians
13 accessed at least one U.S. voting software supplier . . . in most of the targeted states officials saw
14 only preparations for hacking . . . [but] in Arizona and Illinois, voter registration databases were
15 reportedly breached. . . If 2016 was all about preparation, what more can they do and when will
16 they strike? . . . [W]hen asked in March about the prospects for future interference by Russia,
17 then-FBI Director James Comey testified before Congress that: “[T]hey’ll be back. They’ll be
18 back in 2020. They may be back in 2018.”²⁰

19
20
21 ¹⁷ Jordan Robertson and Michael Riley, *The Big Hack: How China Used a Tiny Chip to Infiltrate*
U.S. Companies, Bloomberg (October 4, 2018).

22 ([https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-
chip-to-infiltrate-america-s-top-companies](https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies)).

23 ¹⁸ Ben Popken, Cynthia McFadden and Kevin Monahan, *Chinese parts, hidden ownership,*
24 *growing scrutiny: Inside America's biggest maker of voting machines*, NBC News (Dec. 19,
25 2019) ([https://www.nbcnews.com/news/all/chinese-parts-hidden-ownership-growing-scrutiny-
inside-america-s-biggest-n1104516](https://www.nbcnews.com/news/all/chinese-parts-hidden-ownership-growing-scrutiny-inside-america-s-biggest-n1104516)).

26 ¹⁹ CONGRESSIONAL TASK FORCE ON ELECTION SECURITY, FINAL REPORT (2018)
(<https://homeland.house.gov/imo/media/doc/TFESReport.pdf>).

²⁰ *Id.* at 6-7.

1 95. In a March 21, 2018 hearing held by the Senate Intelligence Committee relating to
2 potential foreign interference in the 2016 election, Senator Ron Wyden warned that:

3 “Forty-three percent of American voters use voting machines that researchers have
4 found have serious security flaws including backdoors. These companies are
5 accountable to no one. They won’t answer basic questions about their cyber security
6 practices and the biggest companies won’t answer any questions at all. Five states
7 have no paper trail and that means there is no way to prove the numbers the voting
8 machines put out are legitimate. So much for cyber-security 101... The biggest
9 seller of voting machines is doing something that violates cyber-security 101,
10 directing that you install remote-access software which would make a machine like
11 that a magnet for fraudsters and hackers.”

12 96. Senator Wyden did not see his concerns addressed. On December 6, 2019, he, along
13 with his Democratic colleagues in Congress – Senator Elizabeth Warren, Senator Amy Klobuchar,
14 and Congressman Mark Pocan – published an open letter concerning major voting system
15 manufacturers. In the letter, they identified numerous problems:

- 16 • “trouble-plagued companies” responsible for manufacturing and maintaining
17 voting machines and other election administration equipment, “have long
18 skimmed on security in favor of convenience,” leaving voting systems across
19 the country “prone to security problems.”
- 20 • “the election technology industry has become highly concentrated ... Today,
21 three large vendors – Election Systems & Software, Dominion, and Hart
22 InterCivic – collectively provide voting machines and software that facilitate
23 voting for over 90% of all eligible voters in the United States.”
- 24 • “Election security experts have noted for years that our nation’s election
25 systems and infrastructure are under serious threat. . . . voting machines are
26 reportedly falling apart, across the country, as vendors neglect to innovate

1 and improve important voting systems, putting our elections at avoidable and
2 increased risk. . . . Moreover, even when state and local officials work on
3 replacing antiquated machines, many continue to ‘run on old software that
4 will soon be outdated and more vulnerable to hackers.’”

- 5 • “[J]urisdictions are often caught in expensive agreements in which the same
6 vendor both sells or leases, and repairs and maintains voting systems-leaving
7 local officials dependent on the vendor, and the vendor with little incentive
8 to substantially overhaul and improve its products.[.]”

9 97. Senator Warren, on her website, identified an additional problem: “These vendors
10 make little to no information publicly available on how much money they dedicate to research
11 and development, or to maintenance of their voting systems and technology. They also share little
12 or no information regarding annual profits or executive compensation for their owners.”

13 98. During a Senate Judiciary Committee hearing in June 2018, then-Senator Kamala
14 Harris warned that, in a demonstration for lawmakers at the Capitol, election machines were
15 “hacked” before the lawmakers’ eyes. Two months later, Senator Klobuchar stated on national
16 television, “I’m very concerned you could have a hack that finally went through. You have 21
17 states that were hacked into, they didn’t find out about it for a year.”

18 99. While chairing the House Committee on Homeland Security in July of 2018,
19 Republican Congressman Michael McCaul decried, “Our democratic system and critical
20 infrastructures are under attack. In 2016, Russia meddled in our Presidential election through a
21 series of cyber attacks and information warfare. Their goals were to undermine the credibility of
22 the outcome and sow discord and chaos among the American people....”

23 100. Senator Wyden stated in an interview, “[T]oday, you can have a voting machine
24 with an open connection to the internet, which is the equivalent of stashing American ballots in
25 the Kremlin. . . . [As] of today, what we see in terms of foreign interference in 2020 is going to
26 make 2016 look like small potatoes. This is a national security issue! . . . The total lack of

1 cybersecurity standards is especially troubling . . . But the lack of cybersecurity standards leads
2 local officials to unwittingly buy overpriced, insecure junk. Insecure junk guarantees three things:
3 a big payday for the election-tech companies, long lines on Election Day, and other hostile foreign
4 governments can influence the outcome of elections through hacks.”

5 101. In March of 2022, White House press secretary Jen Psaki said the Russian
6 government in 2016 “hacked our election here” in the United States.

7 102. The following month, Dara Lindenbaum, a nominee to serve on the Federal Election
8 Commission, testified before the Senate Rules and Administration Committee. Lindenbaum was
9 asked about her role as an election lawyer representing Stacey Abrams’s campaign for governor
10 of Georgia in 2018. Lindenbaum acknowledged she had alleged voting machines were used to
11 illegally switch votes from one candidate to another during the 2018 election in Georgia.²¹

12 103. Dominion presented its Democracy Suite 5.5-A voting system to the State of Texas
13 for certification to be used in public elections in Texas. In January 2019, the State of Texas
14 rejected Dominion’s application and refused to certify Democracy Suite 5.5-A. On October 2 and
15 3, 2019, Dominion presented Democracy Suite 5.5-A to the State of Texas for examination a
16 second time, seeking certification for use in public elections in Texas. Again, Democracy Suite
17 5.5-A failed the test. On January 24, 2020, the Texas Secretary of State denied certification of the
18 system for use in Texas elections.

19 104. The experts designated by Texas to evaluate Democracy Suite 5.5-A flagged risk
20 from the system’s connectivity to the internet despite “vendor claims” that the system is “protected
21 by hardening of data and IP address features,” stating, “[T]he machines could be vulnerable to a
22 rogue operator on a machine if the election LAN is not confined to just the machines used for the
23 election . . . The ethernet port is active on the ICX BMD during an election. . . . This is an
24 unnecessary open port during the voting period and could be used as an attack vector.” Other

25
26 ²¹ PN1758 — Dara Lindenbaum — Federal Election Commission,
<https://www.congress.gov/nomination/117th-congress/1758>;
https://www.youtube.com/watch?v=wCPLL_D_spc

1 security vulnerabilities found by Texas include use of a “rack mounted server” which “would
2 typically be in a room other than a room used for the central count” and would present a security
3 risk “since it is out of sight.” In summary, “The examiner reports identified multiple hardware and
4 software issues Specifically, the examiner reports raise concerns about whether the
5 Democracy Suite 5.5-A system is suitable for its intended purpose; operates efficiently and
6 accurately; and is safe from fraudulent or unauthorized manipulation.”

7 105. The Texas Attorney General explained, “We have not approved these voting
8 systems based on repeated software and hardware issues. It was determined they were not accurate
9 and that they failed — they had a vulnerability to fraud and unauthorized manipulation.”

10 106. Dominion’s DVS 5.5-B voting system, set to be used in the Midterm Election in
11 Arizona, is substantially similar to the 5.5-A system that twice failed certification in Texas.

12 107. Though Texas did certify ES&S electronic voting machines for use in Texas, ES&S
13 voting systems are, like Dominion’s voting systems, opaque, easily hacked, and vulnerable to
14 incorporation of compromised components through ES&S’s supply chain.

15 **E. Electronic Voting Machine Companies Have Not Been Transparent**
16 **Concerning Their Systems**

17 108. Election officials and voting system manufacturers have publicly denied that their
18 election equipment is connected to the internet in order to assert the equipment is not susceptible
19 to attack via a networked system.²²

20 109. John Poulous, the CEO of Dominion Voting Systems, testified in December 2020
21 that Dominion’s election systems are “closed systems that are not networked meaning they are
22 not connected to the internet.” This is false.

23 110. In a May 2016 interview, Dominion Vice President Goran Obradovic stated, “All
24 devices of the ImageCast series have additional options such as modems for wireless and wired
25

26 ²² Kim Zetter, *Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials*, Vice (Aug. 8, 2019) (<https://www.vice.com/en/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials>).

1 transfer of results from the very polling place....”²³ During the 2020 election Dominion election
2 equipment was connected to the internet when it should not have been.²⁴ A Dominion
3 representative in Wayne County, Michigan stated that during the voting in the 2020 election there
4 were irregularities with Dominion’s election equipment, including that equipment was connected
5 to the internet and equipment had scanning issues.

6 111. On Monday, November 2, 2020, the day before the 2020 election, Dominion
7 uploaded software updates into election equipment that Dominion had supplied in the United
8 States.²⁵ These software updates were unplanned and unannounced. In some counties in Georgia,
9 Dominion’s software update caused election equipment to malfunction the next day during the
10 election. The supervisor of one County Board of Elections stated that Dominion “uploaded
11 something last night, which is not normal, and it caused a glitch,” and “[t]hat is something that
12 they don’t ever do. I’ve never seen them update anything the day before the election.” Dominion
13 had earlier publicly denied that any updates just prior to election day were made and that its
14 election equipment was connected to the internet—both of which were false statements.²⁶

15 112. In December 2020, the Department of Homeland Security’s Cybersecurity &
16 Infrastructure Agency (“CISA”) revealed that malicious hackers had compromised and exploited
17 SolarWinds Orion network management software products.²⁷ On April 15, 2021, the White House
18

19 ²³ Economy & Business, Interview: How do the others do this? A technological solution exists
20 for elections with complete security, privacy, and transparency pp.30, 31 (May 2016)
21 ([https://ekonomijaibiznis.mk/ControlPanel/Upload/Free_Editions/wZ0X5bz60KCgpcvFcEBvA/
maj%202016%20ENG/mobile/index.html#p=31](https://ekonomijaibiznis.mk/ControlPanel/Upload/Free_Editions/wZ0X5bz60KCgpcvFcEBvA/maj%202016%20ENG/mobile/index.html#p=31)).

22 ²⁴ Aff. of Patrick J. Colbeck, *Costantino v. City of Detroit*, no. 20-014780-AW (Wayne Co.,
Mich. Cir. Ct. Nov. 8, 2020).

23 ²⁵ Kim Zetter, *Cause of Election Day Glitch in Georgia Counties Still Unexplained*, Politico
(Nov. 12, 2020) ([https://www.politico.com/news/2020/11/04/georgia-election-machine-glitch-
434065](https://www.politico.com/news/2020/11/04/georgia-election-machine-glitch-434065)).

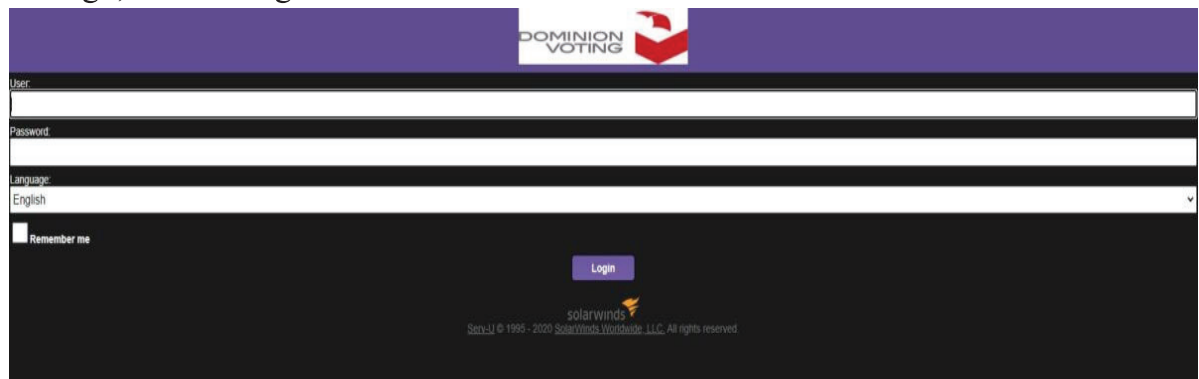
24 ²⁶ Isabel van Brugen, *Dominion Voting Machines Were Updated Before Election, Georgia
25 Official Confirms*, The Epoch Times (Dec. 4, 2020) ([https://www.theepochtimes.com/dominion-
voting-machines-were-updated-before-election-georgia-official-confirms_3604668.html](https://www.theepochtimes.com/dominion-voting-machines-were-updated-before-election-georgia-official-confirms_3604668.html)).

26 ²⁷ CISA, *CISA issues emergency directive to mitigate the compromise of SolarWinds Orion
network management products* (Dec. 14, 2020) ([https://www.cisa.gov/news/2020/12/13/cisa-
issues-emergency-directive-mitigate-compromise-solarwinds-orion-network](https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network)).

1 announced imposition of sanctions on Russia in response to Russian “malicious cyber activities,
2 such as the SolarWinds incident.”²⁸

3 113. Dominion CEO John Poulos stated that Dominion did not use SolarWinds.

4 114. Dominion in fact did use SolarWinds. Dominion’s website formerly displayed a
5 SolarWinds logo, but that logo was removed.



12 115. Dominion refuses to provide access to allow the public to forensically investigate
13 its “proprietary” software, machines, and systems, to determine whether its election equipment is
14 secure, has been hacked, or has malware installed.

15 116. On November 3, 2021, the Tennessee Secretary of State’s office reported to the
16 Election Assistance Commission (EAC) that an “anomaly” was observed during a municipal
17 election in Williamson, County Tennessee, which used Dominion tabulators for a municipal
18 election. This anomaly caused the scanners to mislabel valid ballots as provisional, and therefore
19 did not include these ballots in the poll report totals. After conducting a formal investigation, the
20 EAC concluded the so-called “anomaly” was likely rooted in “erroneous code” present in
21 Dominion’s system. How the “erroneous code” came to be on the voting machine, or how such
22 code was not detected in the certification process or other safety testing procedures, was not
23 included in the investigative report.

24

25 ²⁸ The White House, *Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian*
26 *Government* (Apr. 15, 2021) (<https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/>).

1 117. No electronic voting system to be used in Arizona in the Midterm Election employs
2 “open source” technology, which is electronic equipment for which the details of the components
3 of the system, including its software, is published and publicly accessible. Though Dominion and
4 E&S do not offer open source voting technology, it has been available to Defendants from other
5 vendors for years.

6 118. Defendants have failed or refused to institute open source voting technologies in
7 Arizona, even though such technology would promote both security and transparency, as voters
8 and office-seekers throughout Arizona would know the specific risks to, or manipulation of,
9 election results.

10 119. Open source technology fosters transparency, which is why government agencies
11 have employed it for well over a decade. As the U.S. Department of Defense notes on its website,
12 the following policies apply at the federal level to promote the use of open source programs:

- 13 • The Federal Source Code Policy, OMB Memo 16-21, establishes policy regarding
14 consideration of acquiring custom-developed code, requiring agencies to consider the
15 value of publishing custom code as OSS, and establishing a OSS Pilot Program to release
16 20% of all custom-developed code as OSS. The DoD was later directed to implement this
17 program by Section 875 of the National Defense Authorization Act for FY2018.
- 18 • The DoD CIO issued a memorandum titled “Clarifying Guidance Regarding Open Source
19 Software (OSS)” on 16 October 2009, which superseded a memo May 2003 memo from
20 John Stenbit.
- 21 • The Department of Navy CIO issued a memorandum with guidance on open source
22 software on 5 Jun 2007.
- 23 • The Open Technology Development Roadmap was released by the office of the Deputy
24 Under Secretary of Defense for Advanced Systems and Concepts, on 7 Jun 2006.
- 25 • The Office of Management and Budget issued a memorandum providing guidance on
26 software acquisition which specifically addressed open source software on 1 Jul 2004.

- 1 • US Army Regulation 25-2, paragraph 4-6.h, provides guidance on software security
2 controls that specifically addresses open source software.²⁹

3 120. In 2016, the Obama administration “introduced a new Federal Source Code Policy
4 that called on every agency to adopt an open source approach, create a source code inventory, and
5 publish at least 20% of written code as open source. The administration also launched Code.gov,
6 giving agencies a place to locate open source solutions that other departments are already using.”³⁰

7 121. Earlier this year, the San Francisco Board of Supervisors unanimously passed
8 legislation to authorize the use of open source technologies in the Midterm Election.³¹ San
9 Francisco likely would have done this long ago, were it not for Dominion’s obstruction.

10 122. As reported by the *San Francisco Examiner* in November of last year:

11 “San Francisco’s Elections Department failed to make progress on developing open-
12 source voting technology for more than a decade, while relying heavily on a voting
13 machine company that sees such technology as a threat to its business interests...

14 San Francisco Elections Director John Arntz conferred closely with Dominion
15 Voting Systems, once forwarding the company a city report on open-source voting
16 technology before he had read the report himself...

17 Dominion was the only company to bid on Arntz’s last contract, in which it doubled
18 its rates to \$12 million spread over the next six years.”³²

19 123. Public functions, like voting, should be open to the public. Certain policymakers
20 outside of Arizona understand and have embraced this principle, while Defendants and voting
21 machine companies have shirked it.

22
23 ²⁹ Available at <https://dodcio.defense.gov/open-source-software-faq/#q-what-policies-address-the-use-of-open-source-software-oss-in-the-department-of-defense>.

24 ³⁰ Venky Adivi, *The Stars are Aligning for Federal IT Open Source Software Adoption*,
25 TechCrunch (Aug. 27, 2021) (<https://techcrunch.com/2021/08/27/the-stars-are-aligning-for-federal-it-open-source-software-adoption/>).

26 ³¹ Available at https://sanfrancisco.granicus.com/player/clip/40379?view_id=10&redirect=true

³² Jeff Elder, *San Francisco Pushes Ahead Towards Open-Source Voting Program*, (Nov. 17,
2021) (<https://www.sfxaminer.com/news/san-francisco-pushes-ahead-towards-open-source-voting-program/>).

1 124. This lack of transparency has created a “black box” system of voting which lacks
2 credibility and integrity.

3 **F. Irregularities and Evidence of Illegal Vote Manipulations in Electronic**
4 **Voting Systems During the 2020 General Election Have Been Found**

5 125. Evidence has been found of illegal vote manipulation on electronic voting machines
6 during the 2020 election.

7 126. Dominion Democracy Suite software was used to tabulate votes in 62 Colorado
8 counties, including Mesa County, during the 2020 election. Subsequent examination of equipment
9 from Mesa County showed the Democracy Suite software created unauthorized databases on the
10 hard drive of the election management system servers. On March 21, 2022, electronic database
11 expert Jeffrey O’Donnell and computer science expert Dr. Walter Daugherty published a report
12 concluding that ballots were manipulated in the unauthorized databases on the Mesa County server
13 during Colorado’s November 2020 and April 2021 elections.

14 127. On February 28, 2022, and after a comprehensive review of the Dominion systems
15 used in Colorado, cybersecurity expert Douglas Gould published a report concluding that the
16 system was “configured to automatically overwrite log files that exceed 20 MB, thereby violating
17 federal standards that require the preservation of log files,” that it was configured “to allow any
18 IP address in the world to access the SQL service port, (1433), which violates 2002 VSS security
19 standards,” and that it “uses generic user IDs and passwords and a common shared password,
20 some of which have administrative access,” in violation of 2002 VSS security standards.

21 128. Electronic forensic experts examined equipment used in Michigan to administer
22 voting during the 2020 election and concluded the equipment had been connected to the internet,
23 either by Wi-Fi or a LAN wire, that there were multiple ways the election results could have been
24 modified without leaving a trace; and the same problems have been around for 10 years or more.
25 One expert “examined the forensic image of a Dominion ICX system utilized in the November
26

1 2020 election and discovered evidence of internet communications to a number of public and
2 private IP addresses.”

3 129. In Wisconsin, during the voting in the 2020 election, Dominion election equipment
4 that was not supposed to be connected to the internet was connected to a “hidden” Wi-Fi network.³³

5 130. In April 2021, the Biden administration announced sanctions against Russia for
6 election interference and hacking in the 2020 United States presidential election.³⁴

7 131. Following the 2020 election, lawmakers in multiple states initiated investigations
8 and audits of the results.

9 132. The Arizona Senate hired a team of forensic auditors to review Maricopa County’s
10 election process. The auditors issued a partial audit report on September 24, 2021, which found:
11 (1) “None of the various systems related to elections had numbers that would balance and agree
12 with each other. In some cases, these differences were significant”; (2) “Files were missing from
13 the Election Management System (EMS) Server”; (3) “Logs appeared to be intentionally rolled
14 over, and all the data in the database related to the 2020 General Election had been fully cleared”;
15 (4) “Software and patch protocols were not followed”; and (5) basic cyber security best practices
16 and guidelines from the CISA were not followed.³⁵

17 133. Retired Wisconsin Supreme Court Justice Michael Gableman conducted an
18 investigation of the 2020 election in Wisconsin at the direction of the Wisconsin Assembly.
19 Gableman issued a report in March 2022 noting that “at least some machines had access to the
20 internet on election night.”³⁶ He concluded that several machines manufactured by ES&S and used

21 _____
22 ³³ M.D. Kittle, *Emails: Green Bay’s ‘Hidden’ Election Networks*, Wisconsin Spotlight (Mar. 21,
2021) (<https://wisconsinspotlight.com/emails-green-bays-hidden-election-networks/>).

23 ³⁴ Natasha Truak and Amanda Macias, *Biden administration slaps new sanctions on Russia for*
24 *cyberattacks, election interference*, CNBC (Apr. 16, 2021)
([https://www.cnbc.com/2021/04/15/biden-administration-sanctions-russia-for-cyber-attacks-
election-interference.html](https://www.cnbc.com/2021/04/15/biden-administration-sanctions-russia-for-cyber-attacks-election-interference.html)).

25 ³⁵ *Maricopa County Forensic Election Audit, Volume I*, pp.1-3 (Sept. 24, 2021) (available at
26 [https://c692f527-da75-4c86-b5d1-
8b3d5d4d5b43.filesusr.com/ugd/2f3470_a91b5cd3655445b498f9acc63db35afd.pdf](https://c692f527-da75-4c86-b5d1-8b3d5d4d5b43.filesusr.com/ugd/2f3470_a91b5cd3655445b498f9acc63db35afd.pdf)).

³⁶ Office of the Special Counsel: Second Interim Investigative Report On the Apparatus &
Procedures of the Wisconsin Elections System, March 1, 2022, p. 13.

1 in the 2020 election in Wisconsin were “made with a 4G wireless modem installed, enabling them
2 to connect to the internet through a Wi-Fi hotspot.”

3 134. During a December 30, 2020 live-streamed hearing held by the Georgia Senate
4 Judiciary Subcommittee on Elections, an expert witness testified that an active Dominion polling
5 pad had been hacked and the intrusion was being maintained even as he was speaking.³⁷

6 **G. Arizona’s Voting Systems Do Not Comply with State or Federal Standards**

7 135. All voting systems and voting equipment used in Arizona must comply with
8 standards set forth in Federal Election Commission Publication “2002 Voting Systems Standards”
9 (“2002 VSS”). A.R.S. § 16-442(B).

10 136. The 2002 VSS standards require that all electronic voting systems shall:

- 11 g. Record and report the date and time of normal and abnormal events;
- 12 h. Maintain a permanent record of all original audit data that cannot be
13 modified or overridden but may be augmented by designated authorized
14 officials in order to adjust for errors or omissions (e.g. during the
15 canvassing process.)
- 16 i. Detect and record every event, including the occurrence of an error
17 condition that the system cannot overcome, and time-dependent or
18 programmed events that occur without the intervention of the voter or a
19 polling place operator;

20 [VSS, § 2.2.4.1]

21 ...

- 22 a. Maintain the integrity of voting and audit data during an election, and for
23 at least 22 months thereafter, a time sufficient in which to resolve most
24

25
26 _____
³⁷ Hearing of Georgia Senate Judiciary Subcommittee on Elections, Dec. 30, 2020
(<https://www.youtube.com/watch?v=D5c034r0RIU> beginning at 4:07:58).

1 contested elections and support other activities related to the
2 reconstruction and investigation of a contested election; and

3 b. Protect against the failure of any data input or storage device at a location
4 controlled by the jurisdiction or its contractors, and against any attempt at
5 improper data entry or retrieval.

6 [VSS, § 4.3]

7 137. Defendant Hobbs has statutory duties to test, certify, and qualify software and
8 hardware that is used on county election systems. A.R.S. § 16-442(B). Defendant Hobbs certified
9 Dominion’s DVS 5.5-B voting system for use in Arizona on or around November 5, 2019. The
10 DVS 5.5-B system includes the Dominion ImageCast Precent2 (“ICP2”).

11 138. ICP2 does not meet 2002 VSS standards or Arizona’s statutory requirements. It is
12 normally configured with cellular wireless connections, Wi-Fi access and multiple wired LAN
13 connections, each of which provides an access point for unauthorized remote connection and
14 thereby makes it impossible to know whether improper data entry or retrieval has occurred or
15 whether the equipment has preserved election records unmodified or not, in violation of the
16 standards. The ICP permits software scripts to run which cause the deletion of election log file
17 entries, thereby failing to preserve records of events which the standards require to be recorded.
18 The ICP permits election files and folders to be deleted, in violation of the standards.

19 139. University of Michigan Professor of Computer Science and Engineering J. Alex
20 Halderman performed a thorough examination of voting equipment used in Georgia, which is also
21 used in Arizona. In a series of expert reports submitted in litigation still pending in the Northern
22 District of Georgia, Professor Halderman stated that this voting equipment can be manipulated
23 “to steal votes,” has “numerous security vulnerabilities” that “would allow attackers to install
24 malicious software” through either “temporary physical access (such as that of voters in the
25 polling place) or remotely from election management systems.” He stated that these “are not
26 general weaknesses or theoretical problems, but rather specific flaws” which he was “prepared to

1 demonstrate proof-of-concept malware that can exploit them to steal votes.” He also concluded
2 that the equipment “is very likely to contain other, equally critical flaws that are yet to be
3 discovered.” He specifically noted that this same equipment, the ICX, will be used in 2022 in “for
4 accessible voting in Alaska and large parts of Arizona . . .”

5 140. In the Midterm Election, Arizona intends to use, in part, the same software about
6 which Dr. Halderman testified. The ICX fails to meet VSS standards for the reasons stated in Dr.
7 Halderman’s reports.

8 141. By falling short of VSS standards, DVS 5.5-B is noncompliant with Arizona or
9 federal law and should not have been certified for use.

10 142. By seeking to use DVS 5.5-B in the Midterm Election, Defendant intends to
11 facilitate violations of Arizona law and federal law.

12 143. By choosing to continue using the non-compliant system in the Midterm Election
13 without taking any meaningful steps to remedy known security breaches affecting Arizona voters,
14 Defendants know that they will cause voters to cast votes in Midterm Election on an inaccurate,
15 vulnerable and unreliable voting system that cannot produce verifiable results and does not pass
16 constitutional or statutory muster. Such a system cannot ensure that elections in Arizona,
17 including the Midterm Election, are “free and equal,” as required by Article 2, Section 21 of the
18 Arizona Constitution.

19 **H. Arizona’s Audit Regime is Insufficient to Negate Electronic Voting Machines’**
20 **Vulnerabilities**

21 144. Post-election audits do not and cannot remediate the security problems inherent in
22 the use of electronic voting machines.

23 145. All post-election audit procedures can be defeated by sophisticated manipulation of
24 electronic voting machines.

25 146. Dr. Halderman stated in a Declaration dated August 2, 2021, that malware can defeat
26 “all the procedural protections practiced by [Georgia], including acceptance testing, hash

1 validation, logic and accuracy testing, external firmware validation, and risk-limiting audits
2 (RLAs).” Dr. Halderman testified that the voting system at issue in Georgia is used in fifteen
3 other states, including Arizona.

4 147. Electronic voting systems vendors have repeatedly refused to comply with post-
5 election audits, diminishing the audits’ ability to yield reliable conclusions about the validity of
6 the election results.

7 148. On July 26, 2021, Arizona Senate leaders issued subpoenas to Dominion Voting
8 Systems in connection with the Senate’s audit of the 2020 election in Maricopa County, Arizona.
9 Among other materials, the July 26 subpoenas sought production of usernames, passwords,
10 tokens, and PINs to the ballot tabulation machines the Maricopa County rents from Dominion,
11 including all that would provide administrative access.

12 149. Dominion flatly refused to comply with this validly-issued legislative subpoena. In
13 a letter to Senate President Karen Fann, Dominion wrongly claimed the subpoena seeking
14 credentials necessary to access the Dominion voting systems to validate an election “violat[ed]
15 [Dominion’s] constitutional rights and ... exceed[ed] the Legislature’s constitutional and statutory
16 authority” and that responding to the subpoena would “cause grave harm” to Dominion.

17 150. ES&S has similarly flouted legislative subpoenas in Wisconsin. In a letter dated
18 January 21, 2022, ES&S responded to a Wisconsin subpoena with a letter erroneously asserting it
19 “is under no obligation to respond,” despite the fact the subpoena was issued by the state Senate.

20 151. Any voting system that relies on the hidden workings of electronic devices in the
21 casting and/or counting of the vote is a system of which voters may reasonably be suspicious.
22 Post-election audits are not sufficient to alleviate their reasonable suspicions because voting
23 machine manufacturers have demonstrated that they will not provide the information necessary to
24 audit an election.

25

26

1 152. To restore legitimacy to Arizona’s election regime for all voters, regardless of party,
2 and to comply with constitutional and legal requirements, a secure and feasible alternative must
3 supplant reliance on faulty electronic voting systems.

4 **I. Voting on Paper Ballots and Counting Those Votes by Hand Is the Most**
5 **Effective and Presently the Only Secure Election Method**

6 153. Plaintiffs seek for the Court to Order, an election conducted by paper ballot, as an
7 alternative to the current framework. To satisfy constitutional requirements of reliability,
8 accuracy, and security, the following is a summary of procedures that should be implemented:

- 9 • Ballots are cast by voters filling out paper ballots, by hand. The ballots are then
10 placed in a sealed ballot box. Each ballot bears a discrete, unique identification
11 number, which is made known by election officials only to the voter, so that the
12 voter can later verify whether his or her ballot was counted properly. All ballots will
13 be printed on specialized paper to confirm their authenticity.
 - 14 • Though a uniform chain of custody, ballot boxes are conveyed to a precinct level
15 counting location while still sealed.
 - 16 • With party representatives, ballot boxes are unsealed, one at a time, and ballots are
17 removed and counted in batches of 100, then returned to the ballot box. When all
18 ballots in a ballot box have been counted, the box is resealed, with a copy of the
19 batch tally sheets left inside the box, and the batch tally sheets carried to the tally
20 center with a uniform chain of custody.
 - 21 • Ballots are counted, one at a time, by three independent counters, who each produce
22 a tally sheet that is compared to the other tally sheets at the completion of each
23 batch.
 - 24 • At the tally center, two independent talliers add the counts from the batch sheets,
25 and their results are compared to ensure accuracy.
- 26

- 1 • Vote counting from paper ballots is conducted in full view of multiple, recording,
2 streaming cameras that ensure a) no ballot is ever touched or accessible to anyone
3 off-camera or removed from view between acceptance of a cast ballot and
4 completion of counting, b) all ballots, while being counted are in full view of a
5 camera and are readable on the video, and c) batch tally sheets and precinct tally
6 sheets are in full view of a camera while being filled out and are readable on the
7 video.
- 8 • Each cast ballot, from the time of receipt by a sworn official from a verified, eligible
9 elector, remains on video through the completion of precinct counting and reporting.
- 10 • The video be live-streamed for public access and archived for use as an auditable
11 record, with public access to replay a copy of that auditable record.
- 12 • Anonymity will be maintained however, any elector will be able to identify their
13 own ballot by the discrete, serial ballot number known only to themselves, and to
14 see that their own ballot is accurately counted.

15 154. Every county in Arizona, regardless of size, demographics, or any other ostensibly
16 unique characteristic, can simply and securely count votes cast on paper ballots without using
17 centralized machine-counting or computerized optical scanners.

18 155. The recent hand count in Maricopa County, the second largest voting jurisdiction in
19 the United States, offers Defendant Hobbs a proof-of-concept and a superior alternative to relying
20 on corruptible electronic voting systems. Voting jurisdictions larger than any within Arizona,
21 including France and Taiwan, have also proven that hand-count voting can deliver swift, secure,
22 and accurate election results.

23
24
25 **J. Past and Threatened Conduct of Defendant Hobbs**
26

1 156. Defendant Hobbs is, in her capacity as Secretary of State, charged by statute with
2 carrying out the following duties:

- 3 • “After consultation with each county board of supervisors or other officer in
4 charge of elections, the secretary of state shall prescribe rules to achieve and
5 maintain the maximum degree of correctness, impartiality, uniformity and
6 efficiency on the procedures for early voting and voting, and of producing,
7 distributing, collecting, counting, tabulating and storing ballots.”

8 A.R.S. § 16-452 (A).

- 9 • “The rules shall be prescribed in an official instructions and procedures
10 manual to be issued not later than December 31 of each odd-numbered year
11 immediately preceding the general election. Before its issuance, the manual
12 shall be approved by the governor and the attorney general. The secretary of
13 state shall submit the manual to the governor and the attorney general not
14 later than October 1 of the year before each general election.”

15 A.R.S. § 16-452 (B).³⁸

- 16 • “The secretary of state shall provide personnel who are experts in electronic
17 voting systems and procedures and in electronic voting system security to
18 field check and review electronic voting systems and recommend needed
19 statutory and procedural changes.”

20 A.R.S. § 16-452 (D).

21 157. Defendant Hobbs, in her capacity as Secretary of State, is further charged with
22 ensuring that electronic voting systems used throughout Arizona meet the following requirements:
23
24
25

26 ³⁸ Defendant Hobbs’s failure to timely issue an official instructions and procedures manual is currently the subject of an action brought by Attorney General Brnovich before the Yavapai County Superior Court (case no. P-1300-CV-202200269).

- 1 • “Be suitably designed for the purpose used and be of durable construction,
2 and may be used safely, efficiently and accurately in the conduct of elections
3 and counting ballots...”
- 4 • “When properly operated, record correctly and count accurately every vote
5 cast...” and
- 6 • “Provide a durable paper document that visually indicates the voter’s
7 selections, that the voter may use to verify the voter’s choices, that may be
8 spoiled by the voter if it fails to reflect the voter’s choices and that permits
9 the voter to cast a new ballot.”

10 A.R.S. § 16-446 (B).

11 158. Defendant Hobbs, in her capacity as Secretary of State, is further charged with
12 ensuring that all computer election programs filed with the office of the Secretary of State shall
13 be used by the Secretary of State or Attorney General to preclude fraud or any unlawful act.

14 A.R.S. § 16-445(D).

15 159. By certifying deficient electronic voting systems for use in past elections, Defendant
16 Hobbs has failed to meet these duties set forth above.

17 160. Defendant Hobbs, acting in her official capacity as the Secretary of State, has shown
18 her intention to require the use of electronic voting systems for all Arizona voters in the Midterm
19 Election.

20 161. In so doing, Defendant Hobbs will violate her duties under A.R.S. § 16-442(B), and
21 violate the Constitutional rights of Plaintiffs and all voters in the State of Arizona.

22 **K. Past and Threatened Conduct of Maricopa Defendants and Pima Defendants**

23 162. The Maricopa Defendants and Pima Defendants, acting in their official capacity, are
24 charged with the duty to:
25
26

- 1 • “[e]stablish, abolish and change election precincts, appoint inspectors and
2 judges of elections, canvass election returns, declare the result and issue
3 certificates thereof...”;
- 4 • “[a]dopt provisions necessary to preserve the health of the county, and
5 provide for the expenses thereof”;
- 6 • “[m]ake and enforce necessary rules and regulations for the government of
7 its body, the preservation of order and the transaction of business.”

8 A.R.S. § 11-251.

9 163. The Maricopa Defendants and Pima Defendants, acting in their official capacity, are
10 charged with the duty to consult with Defendant Hobbs in order for Defendant Hobbs to “prescribe
11 rules to achieve and maintain the maximum degree of correctness, impartiality, uniformity and
12 efficiency on the procedures for early voting and voting, and of producing, distributing, collecting,
13 counting, tabulating and storing ballots.” A.R.S. § 16-452 (A).

14 164. The Maricopa Defendants and Pima Defendants have, in the past, failed in the duties
15 set forth above by failing to, among other things, ensure that:

- 16 • operating systems and antivirus definitions of electronic voting systems were
17 properly updated;
- 18 • electronic election files and security logs were preserved;
- 19 • election management servers were not connected to the Internet;
- 20 • access to election equipment was limited to authorized personnel; and
- 21 • communications over the system network were properly monitored.

22 165. The Maricopa Defendants and Pima Defendants intend to rely on the use of deficient
23 electronic voting systems in the Midterm Election.

24 **L. Imminent Injury**

25 166. Plaintiff Lake seeks the office of Governor of the State of Arizona.

26

1 167. To gain that office, Plaintiff Lake must prevail in the Midterm Election, in which
2 all votes will be tabulated, and many votes will be cast, on electronic voting systems.

3 168. Plaintiff Lake intends to vote in the Midterm Election in Arizona. To do so, she will
4 be required to cast her vote, and have her vote counted, through electronic voting systems.

5 169. Plaintiff Finchem seeks the office of Secretary of State of the State of Arizona.

6 170. To gain that office, Plaintiff Finchem must prevail in the Midterm Election, in which
7 all votes will be tabulated, and many votes will be cast, on electronic voting systems.

8 171. Plaintiff Finchem intends to vote in the Midterm Election in Arizona. To do so, he
9 will be required to cast his vote, and have his vote counted, through electronic voting systems.

10 172. All persons who vote in the Midterm Election, if required to vote using an electronic
11 voting system or have their vote counted using an electronic voting system, will be irreparably
12 harmed because the voting system does not reliably provide trustworthy and verifiable election
13 results. The voting system therefore burdens and infringes their fundamental right to vote and
14 have their vote accurately counted in conjunction with the accurate counting of all other legal
15 votes, and *only* other legal votes.

16 173. Any voter who votes using a paper ballot will be irreparably harmed in the exercise
17 of the fundamental right to vote if his or her vote is tabulated together with the votes of other
18 voters who cast ballots using an unreliable, untrustworthy electronic system.

19 174. Any voter will be irreparably harmed in the exercise of the constitutional,
20 fundamental right to vote if he or she is required to cast a ballot using – or in an election in which
21 anyone will use – an electronic voting system, or if his or her ballot is tabulated using an electronic
22 voting system.

23 175. Each of the foregoing harms to Plaintiff is imminent for standing purposes because
24 the Midterm Election is set to occur on a fixed date not later than eight months after the date when
25 this action is to be filed.

26

1 176. No Plaintiff can be adequately compensated for these harms in an action at law for
2 money damages brought after the fact because the violation of constitutional rights is an
3 irreparable injury.

4 **IV. CLAIMS**

5 **COUNT I: VIOLATION OF DUE PROCESS**

6 *(Seeking declaratory and injunctive relief against all Defendants)*

7 177. Plaintiffs incorporate and reallege all paragraphs in this Complaint.

8 178. The right to vote is a fundamental right protected by the Due Process Clause of the
9 Fourteenth Amendment of the U.S. Constitution and Article 2, Section 4 of the Arizona
10 Constitution.

11 179. The fundamental right to vote encompasses the right to have that vote counted
12 accurately, and it is protected by the Due Process Clause of the Fourteenth Amendment of the
13 U.S. Constitution and Article 2, Section 4 of the Arizona Constitution.

14 180. Defendants have violated Plaintiffs' fundamental right to vote by deploying an
15 electronic voting equipment system that has failed:

- 16 • to provide reasonable and adequate protection against the real and substantial threat
- 17 of electronic and other intrusion and manipulation by individuals and entities
- 18 without authorization to do so;
- 19 • to include the minimal and legally required steps to ensure that such equipment
- 20 could not be operated without authorization;
- 21 • to provide the minimal and legally required protection for such equipment to secure
- 22 against unauthorized tampering;
- 23 • to test, inspect, and seal, as required by law, the equipment to ensure that each unit
- 24 would count all votes cast and that no votes that were not properly cast would not
- 25 be counted;
- 26

- 1 • to ensure that all such equipment, firmware, and software is reliable, accurate, and
- 2 capable of secure operation as required by law; and
- 3 • to provide a reasonable and adequate method for voting by which Arizona electors’
- 4 votes would be accurately counted.

5 181. By choosing to move forward in using an unsecure system, Defendants willfully
6 and negligently abrogated their statutory duties and abused their discretion, subjecting voters to
7 cast votes on an illegal and unreliable system – a system that must be presumed to be compromised
8 and incapable of producing verifiable results.

9 182. Despite Defendants’ knowledge that electronic voting systems used in Arizona do
10 not comply and cannot be made to comply with state and federal law, Defendants plan to continue
11 to use these non-compliant systems in the Midterm Election.

12 183. Plaintiffs ask this Court to declare that these Defendants violated the Due Process
13 Clause of the Fourteenth Amendment of the United States Constitution and Article 2, Section 4
14 of the Arizona Constitution; enjoin Defendants’ use of electronic voting systems for future
15 elections; and award attorneys’ fees and costs for Defendants’ causation of concrete injury to
16 Plaintiffs, whose fundamental right to have their vote counted as cast was thwarted.

17 **COUNT II: VIOLATION OF EQUAL PROTECTION**

18 *(Seeking declaratory and injunctive relief against all Defendants)*

19 184. Plaintiffs incorporate and reallege all paragraphs in this Complaint.

20 185. By requiring Plaintiffs to vote using electronic voting systems in the Midterm
21 Election which are unsecure and vulnerable to manipulation and intrusion there will be an unequal
22 voting tabulation of votes treating Plaintiffs who vote in Arizona differently than other, similarly
23 situated voters who cast ballots in the same election.

24 186. These severe burdens and infringements that Defendants will impose unequally on
25 Plaintiffs who vote through an electronic voting system will violate the Equal Protection Clause
26 of the Fourteenth Amendment.

1 187. These severe burdens and infringements that will be caused by Defendants' conduct
2 are not outweighed or justified by, and are not necessary to promote, any substantial or compelling
3 state interest that cannot be accomplished by other, less restrictive means, like conducting the
4 Midterm Election using hand counted paper ballots.

5 188. Requiring voters to be deprived of their constitutional right to equal protection of
6 the laws as a condition of being able to enjoy the benefits and conveniences of voting in person at
7 the polls violates the unconstitutional conditions doctrine.

8 189. Unless Defendants are enjoined by this Court, then Plaintiffs will have no adequate
9 legal, administrative, or other remedy by which to prevent or minimize the irreparable, imminent
10 injury that is threatened by Defendants intended conduct. Accordingly, injunctive relief against
11 these Defendants is warranted.

12 **COUNT III: VIOLATION OF FUNDAMENTAL RIGHT TO VOTE**

13 *(Seeking declaratory and injunctive relief against all Defendants)*

14 190. Plaintiffs incorporate and reallege all paragraphs in this Complaint.

15 191. The right to vote is a fundamental right protected by the U.S. Constitution. *See,*
16 *e.g., Reynolds v. Sims, 377 U.S. 533, 561-62 (1964).*

17 192. The fundamental right to vote encompasses the right to have that vote counted
18 accurately. *See, e.g., United States v. Mosley, 238 U.S. 383, 386 (1915).*

19 193. Defendants have violated Plaintiffs' fundamental right to vote by deploying an
20 electronic voting equipment system that has failed:

- 21 • to provide reasonable and adequate protection against the real and substantial threat
- 22 of electronic and other intrusion and manipulation by individuals and entities
- 23 without authorization to do so;
- 24 • to include the minimal and legally required steps to ensure that such equipment
- 25 could not be operated without authorization;
- 26

- 1 • to provide the minimal and legally required protection for such equipment to secure
- 2 against unauthorized tampering;
- 3 • to test, inspect, and seal, as required by law, the equipment to ensure that each unit
- 4 would count all votes cast and that no votes that were not properly cast would not
- 5 be counted;
- 6 • to ensure that all such equipment, firmware, and software is reliable, accurate, and
- 7 capable of secure operation as required by law; and
- 8 • to provide a reasonable and adequate method for voting by which Arizona electors’
- 9 votes would be accurately counted.

10 194. By choosing to move forward in using the non-compliant system, Defendants have
11 abrogated their statutory duties and abused their discretion, subjecting voters to cast votes on an
12 illegal and unreliable system – a system that is unsecure and vulnerable to manipulation and
13 intrusion and incapable of producing verifiable results.

14 195. Defendants’ violation of the fundamental right to vote is patently and fundamentally
15 unfair and therefore relief is warranted. Accordingly, Plaintiffs ask this Court to declare that these
16 Defendants violated the Due Process Clause of the Fourteenth Amendment of the United States
17 Constitution and Article 2, Section 4 of the Arizona Constitution; enjoin Defendants’ use of
18 electronic voting systems for future elections; and award attorneys’ fees and costs for Defendants’
19 causation of concrete injury to Plaintiffs, whose fundamental right to have their vote counted as
20 cast was thwarted.

21 **COUNT IV: CIVIL ACTION FOR DEPRIVATION OF RIGHTS**

22 **UNDER 42 U.S.C. § 1983**

23 *(Seeking declaratory and injunctive relief against all Defendants)*

24 196. Plaintiffs incorporate and reallege all paragraphs in this Complaint.
25
26

1 206. Unless Maricopa Defendants and Pima Defendants are enjoined by this Court, then
2 Plaintiffs will have no adequate administrative, or other remedy by which to prevent or minimize
3 the irreparable, imminent injury that is threatened by the intended conduct of Maricopa
4 Defendants and Pima Defendants. Accordingly, injunctive relief against these Defendants is
5 warranted.

6 **COUNT VI: DECLARATORY JUDGMENT - 28 U.S. CODE § 2201**

7 *(Against All Defendants)*

8 207. Plaintiffs incorporate and reallege all paragraphs in this Complaint.

9 208. Defendants' conduct will have the effect of violating the rights of the citizens of
10 Arizona, as described above.

11 209. The Court has the authority pursuant to 28 U.S.C. § 2201 to issue an Order declaring
12 that it is unconstitutional for the State of Arizona to conduct an election in which the votes are not
13 accurately or securely tabulated.

14 210. If the State of Arizona is allowed to proceed with an election as described above, it
15 will violate the rights of the citizens of the State by conducting an election with an unsecure,
16 vulnerable electronic voting system which is susceptible to manipulation and intrusion.

17 211. Because of the issues described above regarding the election system to be used by
18 Defendants, the Court should issue an Order declaring that it is unconstitutional for the State to
19 conduct an election which relies on the use of electronic voting systems to cast or tabulate the
20 votes.

21 **PRAYER FOR RELIEF**

22 WHEREFORE, Plaintiffs respectfully request that this Court:

23 1. Enter an Order finding and declaring it unconstitutional for any public election to
24 be conducted using any model of electronic voting system to cast or tabulate votes.

25 2. Enter a preliminary and permanent injunction prohibiting Defendants from
26 requiring or permitting voters to have votes cast or tabulated using any electronic voting system.

1 3. Enter an Order directing Defendants to conduct the Midterm Election consistent
2 with the summary of procedures set forth in paragraph 153 of this Complaint.

3 4. Retain jurisdiction to ensure Defendants' ongoing compliance with the foregoing
4 Orders.

5 5. Grant Plaintiffs an award of its reasonable attorney's fees, costs, and expenses
6 incurred in this action pursuant to 42 U.S.C. § 1988.

7 6. Enter an Order awarding damages suffered by Plaintiffs, to be determined at trial.

8 7. Grant Plaintiff such other relief as the Court deems just and proper.

9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

1 **DEMAND FOR JURY TRIAL**

2 Plaintiffs demand a trial by jury on all counts and issues so triable.

3 DATED: May 4, 2022.

4 **PARKER DANIELS KIBORT LLC**

5 By /s/ Andrew D. Parker
6 Andrew D. Parker (AZ Bar No. 028314)
7 888 Colwell Building
8 123 N. Third Street
9 Minneapolis, MN 55401
10 Telephone: (612) 355-4100
11 Facsimile: (612) 355-4101
12 parker@parkerdk.com

13 **OLSEN LAW, P.C.**

14 By /s/ Kurt Olsen
15 Kurt Olsen (D.C. Bar No. 445279)*
16 1250 Connecticut Ave., NW, Suite 700
17 Washington, DC 20036
18 Telephone: (202) 408-7025
19 ko@olsenlawpc.com

20 * To be admitted *Pro Hac Vice*

21 *Counsel for Plaintiffs Kari Lake
22 and Mark Finchem*

23 By /s/ Alan Dershowitz
24 Alan Dershowitz (MA Bar No. 121200)*
25 1575 Massachusetts Avenue
26 Cambridge, MA 02138

* To be admitted *Pro Hac Vice*

*Of Counsel for Plaintiffs Kari Lake
and Mark Finchem*