UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

US DOMINION, INC., DOMINION VOTING SYSTEMS, INC., and DOMINION VOTING SYSTEMS CORPORATION, *Plaintiffs/Counter-Defendants*, v. MY PILLOW, INC., and MICHAEL J. LINDELL, *Defendants/Counter and Third- Party Plaintiffs,* *v.* SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V., SGO CORPORATION LIMITED, AND HAMILTON PLACE STRATEGIES, LLC, *Third-Party Defendants.*	)	Civil Case No. 1:21-cv-00445 (CJN)

SUPPLEMENTAL MEMORANDUM IN SUPPORT OF DOMINION'S MOTION FOR PROTECTIVE ORDER REGARDING THIRD PARTY SUBPOENAS

In accordance with the Court's order following the January 10, 2023, hearing on Dominion's Motion for Protective Order, Dominion provides this supplemental memorandum in further support of its motion for protective order, which reports on the parties' subsequent meet and confer efforts and provides Dominion's proposal for review of Dominion's confidential and proprietary information.

Dominion moved for protection because Requests 1 and 2(a), which are the heart of Defendants' subpoenas, seek to have Dominion's customers turn over Dominion's confidential

and proprietary information. In light of the Court's instruction during the January 10, 2023, hearing, and after extensive meet and confers with Defendants' counsel, Dominion has accepted, **without revision**, the terms and substance of Defendants' proposal that the counties produce the equipment and software sought in those requests. Dominion does not seek to limit the scope of Requests 1 and 2(a). Dominion simply proposes procedures that allow Defendants to pursue the materials they seek, while adequately protecting Dominions confidential and proprietary materials.

PROCEDURAL HISTORY

In early September, Defendants Michael J. Lindell and My Pillow, Inc. ("Defendants") served substantively identical third-party subpoenas ("the subpoenas") on 39 individual counties throughout the United States. The subpoenas are extraordinarily broad. They request images of all Dominion-manufactured voting equipment and Dominion-created software ("the Dominion equipment and software")[1] that the counties used in the 2020 election, and all documents maintained by each county related to the process and results of the 2020 election. Defendants served the subpoenas without first consulting the counties.

Various counties objected to their subpoenas, and some moved to quash. Those that moved to quash won their motions. Other than opposing the motions to quash and arguing at those hearings, Defendants have not pressed the remaining counties for production of the subpoenaed materials or even confirmed they used Dominion equipment and software in the 2020 election. Because requests 1(a) through 1(h) and 2(a) of the subpoenas call for production of Dominion's confidential and proprietary information without any safeguards, Dominion served Defendants

[1] As identified by Defendants in their subpoenas, "Dominion equipment" comprises Dominion's EMS Server, EMS Client, ImageCast Central Workstations, Adjudication Workstations, Image Cast X, ImageCast Precinct, and ImageCast Evolution used in the 2020 elections. "Dominion software" is the software that was run on those devices. *See* Exhibit A at p.2.

with written objections to those requests and ultimately filed a Motion for Protective Order Regarding Third Party Subpoenas ("the Motion") and a Memorandum in Support of the Motion ("the Memorandum") with this Court [ECF 145]. The Memorandum urged the Court to enter a Protective Order prohibiting Defendants from pursuing Dominion's confidential and proprietary information from third parties and explained that, to the extent Defendants seek to examine the Dominion equipment and software in the form Dominion sold it for the 2020 election, Dominion would be the proper party from which to pursue those materials. Defendants nevertheless insisted on pursuing Dominion's confidential and proprietary equipment and software from Dominion's customers and opposed the Motion [ECF 147]. Dominion filed a reply [ECF 152].

In December, while the Motion remained pending, the Court entered a protective order ("the Order") applicable broadly to all materials produced in the case [ECF 152]. Among other things, the Order prohibits anyone from using Discovery Material outside of these cases for any purpose.

Shortly after entering the Order, the Court entered a separate minute order requesting additional briefing from the parties on the effect of the Order on Dominion's pending Motion [ECF Unnumbered (dated 12/08/2022)].

The Parties briefed the issue [ECF 153-156].[2] The Court conducted a thorough hearing on January 10, 2023. During the hearing, the Court asked Defendants to identify how the information the subpoenas request is relevant to their defense of Dominion's defamation claim.[3] Defendants

[2] The Order in this case allows this Court to impose "additional safeguards with respect to the use and handling of Discovery Material." *See* ECF 152 ¶¶ 17, 18(c). In other words, the existence of the current Order does not prohibit or determine the resolution of this request.

[3] Early in the litigation, Defendants filed a counterclaim with allegations that Dominion's equipment is generally vulnerable to hacking [ECF 90]. The Court dismissed Defendants' counterclaim on May 19, 2022, removing the issue from the case [ECF 135, 136].

responded that it is relevant to proving the truth of one of the 24 statements Dominion alleges Lindell made that were false and defamatory: that China hacked Dominion equipment on election night. Based on that representation, the Court concluded that Defendants are entitled to discovery into whether, in fact (as opposed to in theory), the statement is false.

The parties then generally discussed whether the requests are tailored to prove that China did hack Dominion equipment and software. Dominion argued that the requests are not so limited and better, less intrusive, and less burdensome ways exist for Defendants to obtain that information. Defendants argued that Dominion's suggested alternatives are inadequate and took issue with Dominion's explanation of what the process of obtaining the information they requested entails. Both arguments included technical discussions about hacking and voting machinery.

At the conclusion of the hearing, the Court noted its discomfort with adopting one or the other parties' representations as to how voting equipment works and the burden and risks associated with responding to the subpoenas. It concluded, however, that the subpoenas were overbroad as drafted. The Court therefore ordered the parties to "make a good faith effort to narrow the set of information requested of the counties" and follow up with competing proposals if those discussions were not fruitful ("the Meet and Confer Order") [ECF unnumbered (dated 01/10/2023)].

In the last two weeks, the parties have met and conferred three times for a total of approximately 5 hours. The majority of the meet and confer process focused on requests 1 and 2(a)—those to which Dominion objected. Because Dominion could not suggest ways to narrow the requests without knowing their scope, and also understanding how the information and forensic images could theoretically prove the truth (or not) of Mr. Lindell's statement, the parties spent much of the first call discussing those issues. Most specifically, Dominion asked Defendants to

explain what Lindell meant when he said the Dominion machines were "hacked"—a term the subpoenas do not define—and what computer drives Defendants maintain are "affiliated with" the Dominion equipment and software, including whether they include non-Dominion equipment.

Defendants did not, or were not able to, answer most of the questions with anything other than broad generalities. But after much discussion, Defendants conveyed, essentially, that "hacked" includes any physical or electronic incursion by anyone either directly into any Dominion software or equipment, or indirectly through "affiliated" drives. Affiliated drives, in turn, includes non-Dominion equipment or software that communicates in any way with Dominion software or equipment, including malware loaded onto a non-Dominion machine that "hacks" the Dominion equipment or software without leaving any trace. When asked what specific equipment and software counties use to communicate with Dominion machines, Defendants responded that they would not know until they talked with the counties—which they had not done. Given the breadth of those definitions, Defendants took the position that all materials requested in 1 and 2(a) are essential and refused to consider modifying the objected-to subpoena requests in any way. Moreover, Defendants rejected Dominion's proposals that they limit the scope of their requests to Dominion equipment and software and only to Dominion equipment and software in the same condition as it existed in 2020.

During the second meet and confer, Defendants orally offered a limiting proposal. Because the language of the proposal differed (to some extent) from the language of the subpoenas, Dominion asked Defendants, section by section, whether the proposal changed in any way what requests 1(a) through (h) and 2(a) call for. Defendants confirmed that their proposal did not eliminate or narrow any of those requests.

Dominion also delved further into the questions of what, exactly, Defendants intended to use the information to prove and why they couldn't limit the information to Dominion equipment and software. The only substantive answer Defendants provided was the "disappearing" malware theory. When Dominion questioned the logic behind the argument that malware that destroys itself on Dominion equipment would not also destroy itself on the non-Dominion equipment, Defendants claimed that their experts assured them it might still be possible to find "traces" of the malware in the non-Dominion equipment. Defendants likewise argued that none of the equipment or software—Dominion or non-Dominion—needed to be in the state they existed at the time of the 2020 election because, likewise, their experts said that even modified equipment and software might still contain some information from the 2020 election that might bear on the issue of whether the machines were hacked in 2020.[4]

Defendants therefore once again rejected the offers Dominion made in the prior meet and confer (only Dominion equipment and software, only as it existed in 2020). In other words, Defendants held firm as to the breadth and substance of their requests for Dominion's confidential and proprietary information and non-Dominion equipment and software.

The meet and confer did accomplish something, however. The parties were able to agree on four process points: (i) a certified and independent laboratory would gather the images at each county so as not to destroy the existing certifications of the equipment and software being imaged; (ii) Dominion and Defendants can be present during the imaging process, if they choose; (iii) given the cost and time involved in the proposed process, Defendants will consider limiting the number

[4] Dominion does not agree that either theory is valid. In fact, Dominion adamantly contends that they are not, and that the entire process that Defendants plan to engage in will be needlessly expensive, time consuming, and ineffective at demonstrating the existence of a hack by the Chinese government.

of counties for which they would enforce the subpoenas (although they did not give any number or concrete proposal and still have not); and (iv) because Defendants had chosen this approach to discovery, they would either pay for the process or request that the counties participate in payment, but would not ask Dominion to participate except to pay for copies of forensic images Dominion received.

Defendants also represented that they would be conferring with the counties individually to determine what equipment and software is covered by their proposal and then negotiate what the county would agree to produce.

Defendants reduced their "new" proposal—the one that did not modify requests 1(a) through (h) and 2(a) in any way—to writing on the morning of the parties' last meet and confer. By that time, Dominion understood that Defendants were not going to agree to provide more explanation as to what constitutes a "hack" or how "hacks" of Dominion equipment and software could be discerned from non-Dominion equipment and software when they cannot be found in the Dominion equipment and software that was allegedly hacked. Dominion also understood that Defendants would not agree to limit the scope of their requests 1(a) through (h) and 2(a).

Given Defendants' consistent stand on these issues through both calls, and their rejection of Dominion's proposals, Dominion received permission from its client that day to change approach on the upcoming call. On the call, Dominion confirmed with Defendants that Defendants would image only "non-Dominion" equipment that communicated during the 2020 election with the Dominion equipment or software. ***Dominion then accepted, without revision, the terms and substance of Defendants' proposal that the counties produce the equipment and software requested in 1(a) through (h) and 2(a)***. Instead, of trying to narrow the substance of Defendants' requests, Dominion simply proposed additional procedural safeguards to the process, as the Order

expressly permits, to further protect against disclosure of Dominion's confidential and proprietary information. Defendants summarily rejected the proposal on the call, including provisions to which they previously agreed, except that they accepted the provision that a certified neutral lab would gather the images. According to Defendants, they rejected the remaining parts of Dominion's procedural proposal on the grounds that procedures should be negotiated separately between each county and Defendants and, as a non-party to the subpoenas, Dominion has no interest in those procedures. Defendants' argument is obviously wrong. The entire purpose behind Dominion's Motion was to ensure that its confidential and proprietary information is appropriately safeguarded. Dominion clearly has an interest in the procedure governing the gathering and protection of that information. Dominion's proposal follows.

PROPOSAL

1. Defendants will choose which counties to approach about imaging Dominion equipment and software and non-Dominion equipment and software that communicated with the Dominion equipment and software ("the Imaging"). They may approach as few or as many counties as they like.
2. For each county Defendant chooses, and before embarking on the Imaging, Defendants will obtain a certification from the county that (i) the county used Dominion equipment and software during the 2020 presidential election, and (ii) the Dominion equipment and software, and any non-Dominion equipment or software that communicated with the Dominion equipment and software, exist in the same form and condition that they existed in the 2020 election ("the Equipment and Software").[5]

[5] If the Court adopts Dominion's approach, Dominion will provide a certification form acceptable to Dominion within two business days.

3. The parties will agree on a neutral third-party lab to conduct the forensic imaging of the Equipment and Software ("the Neutral"). Dominion suggests the EAC Certified Lab, which conducted the post-election review process in Maricopa County, or Idaho National Lab, which CISA uses.
4. Representatives from either side may be present during any imaging.
5. The Neutral will keep a log of the Equipment and Software imaged at each county and provide a copy to each party.
6. The Neutral will deliver the Imaging to the offices of Dominion's counsel at Susman Godfrey in Houston, Texas, for safeguarding. Susman Godfrey will maintain the Imaging in a secure location and make it available to Defendants for review during working hours.
7. Susman Godfrey will also provide Defendants' representatives with a private office to work from during breaks in the review process.
8. Defendants will not duplicate or otherwise provide the Imaging to any person during the review process. As such, Defendants will not be permitted internet access while reviewing the Imaging and will leave their phones outside the room. Susman Godfrey has the right to monitor compliance with this paragraph.

The purposes behind these certifications are readily apparent. So far, Defendants have not asked any county whether they used Dominion equipment and software in the 2020 election. Nor have they explained how they chose the specific counties they subpoenaed. In fact, one county defeated Defendants' subpoena in part because it did not use the particular equipment during the 2020 election that Defendants seek. Without the certification, therefore, the process of imaging could be a worthless and deceptive exercise. Undoubtedly it would complicate discovery and, potentially, trial.

Dominion's request for certification that the Equipment and Software exist in the same form and condition as they existed in the 2020 election serves the same purpose. Subsequent changes defeat Defendants' ability to prove that the Equipment or Software affected the results of the 2020 election, the only election relevant to this lawsuit. That is why Defendants acknowledged to the Florida court that heard Monroe County's motion to quash that they were seeking images of the drives as they existed immediately following the 2020 general election. In that case, the Supervisor could not represent that those still existed.

9. If Defendants determine that any part of the Imaging discloses or could disclose a potential hack, they shall identify that part of the Imaging for the Neutral or any agreed-upon third-party, who will create a copy of the relevant Imaging for each of Defendants and Dominion, which shall be provided to both simultaneously.
10. All Imaging, including any provided to Defendants, will be treated as AEO under the existing protective order in this case.
11. Once Defendants' review is completed, the Neutral or other agreed-upon third-party will transport to and maintain the Imagining at a secure location.
12. If Dominion decides to review the Imaging, the Neutral or other agreed-upon third-party will transport the Imaging back to Susman Godfrey. If the Neutral or other agreed-upon third-party copies portions of the Imaging at Dominion's request, they shall provide copies to Defendants and Dominion simultaneously.
13. If either party later determines that it requires additional access to the Imaging in order to respond to arguments from the other side, the parties will follow the procedures set forth above in conducting their reviews.
14. The Imaging will be destroyed when and according to the procedures set forth in the Order.
15. Dominion will not charge Defendants for the use of Susman Godfrey's offices. Dominion will pay for any copies of the Imaging it receives but will not be responsible for paying any other costs.

Dated: January 27, 2023

Respectfully submitted,

/s/ Laranda Walker

Justin A. Nelson (D.C. Bar No. 490347)
Katie Sammons (D.C. Bar No. TX0030)
Laranda Walker (D.C. Bar No. TX0028)
Florence T. Chen (D.C. Bar No. TX0025)
SUSMAN GODFREY LLP
1000 Louisiana Street, #5100
Houston, Texas 77002
(713) 651-9366
jnelson@susmangodfrey.com
lwalker@susmangodfrey.com
fchen@susmangodfrey.com
ksammons@susmangodfrey.com

Stephen Shackelford, Jr.
(D.C. Bar No. NY0443*)*
Elisha Barron (*admitted pro hac vice*)
SUSMAN GODFREY LLP
1301 Avenue of the Americas, 32nd Fl
New York, NY 10019
(212) 336-8330
sshackelford@susmangodfrey.com
ebarron@susmangodfrey.com

Davida Brook (D.C. Bar No. CA00117*)*
SUSMAN GODFREY LLP
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
(310) 789-3100
dbrook@susmangodfrey.com

Thomas A. Clare, P.C. (D.C. Bar No. 461964)
Megan L. Meier (D.C. Bar No. 985553)
Dustin A. Pusch (D.C. Bar No. 1015069)
CLARE LOCKE LLP
10 Prince Street
Alexandria, VA 22314
Telephone: (202) 628-7400
tom@clarelocke.com
megan@clarelocke.com
dustin@clarelocke.com

Rodney Smolla (Bar No. 6327)
4601 Concord Pike
Wilmington, DE 19803

rodsmolla@gmail.com
(864) 373-3882

Attorneys for Plaintiffs/Counter-Defendants US Dominion, Inc., Dominion Voting Systems, Inc., and Dominion Voting Systems Corporation; and Third-Party Defendant Hamilton Place Strategies, LLC