UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

My Pillow, Inc. DBA MyPillow,

Plaintiff,

v.

US DOMINION, INC., DOMINION VOTING SYSTEMS, INC., and DOMINION VOTING SYSTEMS CORPORATION,

Defendants.

Court File No. _____

COMPLAINT
WITH DEMAND FOR JURY TRIAL

I. INTRODUCTION

1. Freedom of speech, and free and fair elections, are twin pillars of our constitutional order. Intersection of the two—debate in the public square about elections—is therefore a matter of grave constitutional concern. Discussion of election integrity must receive the highest protection under the First Amendment.

2. Defendants (referred to herein collectively as "Dominion") have engaged in a scorched earth campaign, debasing the legal system through a practice that has become known as "lawfare." Dominion's purpose is to silence debate; to eliminate any challenge to the 2020 presidential election; and to cancel and destroy anyone who speaks out against Dominion's work on behalf of the government in administering the election.

3. Evidence of problems with electronic voting systems, including Dominion's system, has been accumulating for over a decade, and the 2020 election cycle only

accelerated this trend. Prior to 2020, it was well-established that these systems are wide-open to hacking. Evidence that Dominion's voting systems actually were hacked in the 2020 election continues to accumulate. Questions and concerns are growing, not subsiding. The adverse impact of electronic voting systems on the 2020 election was significant. A prudent, robust democracy cannot afford to ignore this evidence if it hopes to survive.

4. Some states, like Texas, rejected Dominion voting systems after examining their vulnerability to hacking. Others, like Arizona, have found cause to order post-election forensic audits of electronic voting systems—including Dominion's voting machines—to attempt to "restore integrity to the election process."[1] Last month, the New Hampshire Senate voted 24-0 to conduct a complete examination of Dominion-owned voting machines after suspicious shorting of votes was discovered.[2] Litigation involving Dominion's voting machines is ongoing in Antrim County, Michigan after about 6,000 votes were discovered to have been wrongly switched between Presidential candidates—a so-called "glitch."[3] During a December 30, 2020 live-streamed hearing held by the Georgia Senate Judiciary

[1] Press Release, Ariz. Senate Republicans, Senate chooses qualified auditing firm to conduct forensic audit of Maricopa County election results (Jan. 29, 2021) https://www.azsenaterepublicans.com/post/senate-chooses-qualified-auditing-firm-to-conduct-forensic-audit-of-maricopa-county-election-results.

[2] Chad Groenig, *Dominion gets caught shorting GOP candidates*, One News Now, Mar. 5, 2021, https://onenewsnow.com/politics-govt/2021/03/05/dominion-gets-caught-shorting-gop-candidates.

[3] Tom Pappert, *VIDEO: Michigan County Discovers 'Glitch' That Gave 6,000 Trump Votes to Biden*, National File, Nov. 6, 2020, https://nationalfile.com/video-michigan-county-discovers-glitch-that-gave-6000-trump-votes-to-biden/; Jack Windsor, *Votes for Trump Went to Biden in Antrim County, Michigan*, The Michigan Star, Nov. 7, 2020, https://themichiganstar.com/2020/11/07/votes-for-trump-went-to-biden-in-antrim-county-michigan/.

Subcommittee on Elections, a testifying expert hacked into a Dominion polling pad during a live broadcast to the world.[4]

5. MyPillow's founder and CEO has spoken in his personal capacity accurately about these issues of great public concern. He has presented evidence backed by expert analysis to raise public awareness of election integrity issues—particularly relating to the hacking of electronic voting machines like Dominion's machines. For those actions, Dominion sued him baselessly alleging defamation and seeking a headline grabbing, fictitious $1.3 billion in damages.

6. However, Dominion's true purpose is not simply to silence Mike Lindell, but to silence anyone else who might speak out on election fraud. Thus, Dominion also sued the company Mike Lindell founded, MyPillow, and hence its hundreds of employees, some of whom are co-owners. Dominion did not sue MyPillow because MyPillow made statements about Dominion. MyPillow made no such statements. Instead, by suing MyPillow, Dominion seeks to punish MyPillow's CEO, Mike Lindell, for *his* statements. Dominion also seeks to send a message to others: "Shut up or else."

7. That is why Dominion's campaign also included bragging publicly about sending threatening letters to over 150 individuals demanding they cease and desist from commenting on the election or Dominion.[5] Among the recipients of these shotgun-style

[4] Ski, *Dominion machines hacked LIVE during Georgia election hearing*, Blue White Illustrated (Dec. 30, 2020, 10:31 AM), https://bwi.forums.rivals.com/threads/dominion-machines-hacked-live-during-georgia-election-hearing.286325/.

[5] Hannah Knowles and Emma Brown, *Dominion threatens MyPillow CEO Mike Lindell with lawsuit over 'false and conspiratorial' claims*, Washington Post, Jan. 18,

attack letters are everyday citizens—not public figures—who volunteered as poll watchers in the 2020 election and signed sworn statements about election irregularities they witnessed. Dominion found out who they were and dispatched its lawyers to send them threatening cease-and-desist letters, falsely claiming they had defamed Dominion when these private citizens never mentioned Dominion. Dominion then illegally demanded these private citizens preserve all communications, emails, texts—private or otherwise—and a host of other materials. Dominion's and its lawyers' widespread intimidation tactics of ordinary citizens may be routine in a Third World country—but they are abhorrent in America. "[T]here is no justification for harassing people for exercising their constitutional rights." *Bart v. Telford*, 677 F.2d 622, 625 (7th Cir. 1982).

8. However, Dominion did not stop there. To give its letters further intimidating weight, Dominion's campaign extended to suing several news networks, like Fox News, and individuals for billions of dollars. These lawsuits were amplified by a high-powered, well-orchestrated publicity campaign designed to spread their allegations to as many people as possible. Dominion intends for its media blitzkrieg to inflict a crippling fear of becoming the next target for destruction if one dares to raise any question about the use and integrity of voting machines during elections.

9. In a highly publicized interview, Dominion's CEO threatened that the lawsuit Dominion brought against MyPillow was "definitely not the last" lawsuit and that Dominion is "not ruling anyone out." Dominion's message is clear: be silent and fall in

---

2021, https://www.washingtonpost.com/politics/2021/01/18/dominion-mike-lindell-mypillow/.

line—or you will be next to be taken down under its relentless attack. Harkening back to some of the worst days in our history, Dominion has taken a page out of Joseph McCarthy's playbook by creating a blacklist for public scorn leading to both reputational and economic destruction. From high-powered news organizations to regular citizens and private home-bedding companies, no one is safe.

10. Having never commented on the election or Dominion, MyPillow has nonetheless borne the full wrath of Dominion's illegal campaign of intimidation. By this action, MyPillow seeks to hold Dominion accountable for the extreme and destructive consequences of its bullying and wrongful tactics which have directly harmed MyPillow and its employees.

11. Far beyond harassment, MyPillow has been intentionally targeted and greatly damaged by Dominion. MyPillow employees live in fear. Their lives have been threatened. They have been canceled and shut down. They have been compelled to self-censor. In addition, MyPillow has lost numerous major customers who ended their long-term relationships to sell MyPillow's product line due to Dominion's highly publicized attacks.

12. Dominion is using the legal process as a weapon to suppress free speech. In contrast, MyPillow brings this action to *open* debate and *expand* free speech. Indeed, MyPillow would move this entire debate to the public square for a full airing of all facts and opinions on the subject. This lawsuit is brought in support of the marketplace of ideas and to remedy the grave harm that has been suffered by MyPillow as a result of Dominion's suppression of speech and attacks on the Company.

II. PARTIES

13. Plaintiff My Pillow, Inc. DBA MyPillow ("MyPillow") is a Minnesota corporation with its principal place of business in Chaska, Minnesota.

14. Defendant US Dominion, Inc. is a Delaware corporation with its principal place of business in Denver, Colorado.

15. Defendant Dominion Voting Systems, Inc. is a Delaware corporation with its principal place of business in Denver, Colorado.

16. Defendant Dominion Voting Systems Corporation is an Ontario corporation with its principal place of business in Toronto, Ontario.

17. Defendants are referred to herein collectively as "Dominion."

III. JURISDICTION AND VENUE

18. Jurisdiction in this matter arises under 28 U.S.C. § 1331. Plaintiff brings claims under laws of the United States. Supplemental jurisdiction over Plaintiff's Minnesota state law claims arises under 28 U.S.C. § 1367(a). The state law claims are so related to the federal law claims as to form part of the same case or controversy. Jurisdiction also arises under 28 U.S.C. § 1332 because there is complete diversity of citizenship between Plaintiff and the Defendants, and the amount in controversy exceeds $75,000, exclusive of interest and costs.

19. Venue is proper in the District of Minnesota pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in Minnesota and Plaintiff's domicile and operations are in Minnesota. Plaintiff also has suffered damages in Minnesota resulting from Defendants' actions.

20. This Court has personal jurisdiction over Defendants because Defendants transact business within Minnesota. Defendants' voting machines and services are used in Minnesota. Defendants have sold their products and services within (and to) Minnesota. Defendants purposely avail themselves of numerous benefits and privileges of Minnesota law. Requiring Defendants to litigate these claims in Minnesota does not offend traditional notions of fair play and substantial justice and is permitted by the Due Process Clause of the United States Constitution.

IV. FACTUAL ALLEGATIONS

A. Dominion provides election administration services and equipment.

21. Dominion manufactures, distributes, and maintains voting hardware and software. Dominion executes software updates, fixes, and patches for its voting machines, including as late as the night before election day, and it pushes out such software through means selected at its own discretion, including via the internet.

22. Dominion designs public election processes with its hardware and software products at the center and provides administrative services for public elections. While polls are open, Dominion employees stand by to provide troubleshooting and support when voting machines malfunction, among other election services. Dominion audits the performance of the machines and elections.

B. Dominion administers elections across the United States.

23. For the 2020 election, Dominion provided its voting machines and services in more than half of the United States, including Minnesota. Many of these states, such as Arizona, Nevada, Wisconsin, Michigan, Georgia, Florida, and Pennsylvania, have been

referred to as battleground or swing states because their voters are equally divided (or nearly equally divided) in their degree of support for the two primary political parties. Dominion has contracts with over 1,300 governmental jurisdictions around the United States to administer elections.

C. Dominion is a governmental actor.

24. As a result of Dominion's contracts with government entities, it is delegated responsibility to administer public elections—a core governmental function.

25. By its own account Dominion provides an "END-TO-END ELECTION MANAGEMENT SYSTEM" that "[d]rives the entire election project through a single comprehensive database."[6] Its tools "build the election project," and its technology provides "solutions" for "voting & tabulation," and "tallying & reporting," and "auditing the election." The products sold by Dominion include ballot marking machines, tabulation machines, and central tabulation machines, among others.

26. By contracting with governmental jurisdictions to provide comprehensive voting solutions for public elections, including the election of individuals to serve in constitutionally prescribed offices, and as more fully described herein, Dominion is a governmental actor.

27. Dominion's involvement in running the presidential election amounts to state action. Dominion willfully participates in joint activity with the state during voting,

[6] DEMOCRACY SUITE® ELECTION MANAGEMENT SYSTEM, https://www.dominionvoting.com/democracy-suite-ems/ (last visited Apr. 18, 2021).

including by supplying its products and services coextensively with election officials to carry out the election. There is pervasive entwinement between Dominion and the state.

28. In its capacity as—and using its authority as—a governmental actor, Dominion allowed manipulation or changing of votes in the 2020 election, as well as suppressed public debate about the election which deprived MyPillow of its rights.

29. As a result of systemic and widespread vulnerabilities in Dominion's software and hardware, widespread claims have been lodged that during the 2020 election significant numbers of votes across the country were altered.

D. Well before the 2020 election, a broad spectrum of evidence showed Dominion's voting machines were wide open to being hacked, and a multitude of government officials and media sources publicized this vulnerability.

30. For many years serious security and technology problems have dogged Dominion's election machines and systems.

31. In May 2010, Dominion purchased Premier Election Solutions ("Premier") from Election Systems & Software ("ES&S"), thereby acquiring all intellectual property, software, and firmware and hardware for Premier's voting systems and all versions of Premier's Global Election Management System (GEMS). [7]

32. Premier was formerly owned by Diebold Elections Systems, but its name was changed from Diebold in 2007 after a series of studies publicized Diebold's unreliable security and accuracy, and technical problems sullied its reputation. The name change was

[7] "Dominion Voting Systems, Inc. Acquires Premier Election Solutions Assets from ES&S" (May 20, 2010), available at https://www.benzinga.com/press-releases/10/05/b292647/dominion-voting-systems-inc-acquires-premier-election-solutions-assets-.

motivated by the desire to create a fresh public image.[8] Then, in September 2009, parent company Diebold sold Premier to ES&S for $5 million, reporting a $45 million loss.[9] About nine months later ES&S sold Premier to Dominion, in May 2010.

33. The Diebold technology Dominion obtained when it acquired Premier had a long and troubled track record.

a. In 2003, it was discovered that Diebold had left approximately 40,000 files that made up its foundational e-voting security software code, GEMS, entirely unprotected on a publicly accessible website.[10]

b. Following the discovery that the GEMS code was publicly available, computer programmers around the world began probing and testing it. In 2012, a Harper's Magazine article titled "How to Rig an Election" summarized, "GEMS turned out to be a vote rigger's dream. According to [one investigator's] analysis, it could be hacked, remotely or on-site, using any off-the-shelf version of Microsoft Access, and password protection was missing for supervisor functions. Not only could multiple users gain access

[8] Allison St. John, *Diebold Voting Machine Company Changes Name to Improve Image*, KPBS (Aug. 21, 2007) available at https://www.kpbs.org/news/2007/aug/21/diebold-voting-machine-company-changes-name-to/.
[9] Ryan Paul, *Diebold impeaches e-voting unit, sells it off for $5 million*, ARS TECHNICA (Sept. 4, 2009), available at https://arstechnica.com/tech-policy/2009/09/diebold-elects-to-get-out-of-the-voting-machine-business/.
[10] Victoria Collier, *How to Rig an Election*, HARPER'S MAGAZINE (Nov. 2012), available at https://harpers.org/archive/2012/11/how-to-rig-an-election/.

to the system after only one had logged in, but unencrypted audit logs allowed any trace of vote rigging to be wiped from the record."[11]

c. In 2004, a team of computer scientists from Johns Hopkins University and Rice University concluded about the GEMS code: "this voting system is far below even the most minimal security standards applicable in other contexts . . . . [It] is unsuitable for use in a general election." [12] More broadly, the team wrote, "The model where individual vendors write proprietary code to run our elections appears to be unreliable, and if we do not change the process of designing our voting systems, we will have no confidence that our election results will reflect the will of the electorate. We owe it to ourselves and to our future to have robust, well-designed election systems to preserve the bedrock of our democracy."

d. In 2006, a team of computer scientists at Princeton University analyzed the security of the Diebold AccuVote-TS voting machine, then one of the most widely-deployed electronic voting platforms in the United States. They found, "Malicious software running on a single voting machine can steal votes with little risk of detection. The malicious software can modify all of the records, audit logs, and counters kept by the voting machine, so that even

[11] *Id*.

[12] Takayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, *Analysis of an Electronic Voting System, IEEE Symposium on Security and Privacy and Privacy 2004*, IEEE COMPUTER SOCIETY PRESS, May 2004, available at https://avirubin.com/vote.pdf (Ex. 1).

careful forensic examination of these records will find nothing amiss. . . . Anyone who has physical access to a voting machine, or to a memory card that will later be inserted into a machine, can install said malicious software using a simple method that takes as little as one minute. . . . AccuVote-TS machines are susceptible to voting machine viruses – computer viruses that can spread malicious software automatically and invisibly from machine to machine during normal pre- and post-election activity."[13]

e. The Princeton team prepared a video demonstration showing how malware could shift votes cast for one candidate to another.[14] In the video, mock election votes were cast in favor of George Washington by a 4 to 1 margin, but the paper print-out that reported the results showed Benedict Arnold prevailing by a margin of 3 to 2. Malicious vote-stealing malware was the sole reason for reallocation of votes from Washington to Arnold, and the malware deleted itself after the election, leaving no evidence that the voting machine was ever hijacked or any votes stolen.[15]

34. Despite the multitude of security weaknesses in GEMS, the "vote rigger's dream," Dominion wasted no time incorporating GEMS into its voting machines after

[13] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine*, USENIX (Sep. 13, 2006), https://www.usenix.org/legacy/event/evt07/tech/full_papers/feldman/feldman_html/index.html (Ex. 2).
[14] *See Security Demonstration of DieBold AccuVote-TS Electronic Voting Machine*, YOUTUBE (Nov. 30, 2016) https://www.youtube.com/watch?v=B8TXuRA4IQM&t=20s.
[15] *See id*.

acquiring the technology in 2010. By 2011, Dominion Voting Systems was selling voting systems that had updated GEMS software at their heart.[16]

35. Even before Dominion acquired the GEMS system, Dominion's machines were riddled with problems globally. In 2009, during a New York congressional election, Dominion's software had problems including that it allowed voters to vote for more than one candidate, and its faulty machines froze during operation due to insufficient memory.[17] In 2010, in a Philippines election where Dominion's products were in more than 2,200 local municipalities, a Dominion glitch caused voting machines to incorrectly read ballots. A Product Manager of Dominion indicated that more than 76,000 compact flash cards had to be configured just days before the election.[18]

36. Dominion continued selling and leasing the troubled AccuVote voting machine as recently as 2017.[19]

37. Dominion voting systems reliant on GEMS were used in the 2020 general election.

---

[16] Ken Detzner, *Voting System Qualification Test Report Dominion Voting Systems, Inc. GEMS Release 1.21.6, Version 1*, FLA. DEP'T OF STATE (Mar. 2012), https://files.floridados.gov/media/697908/dominion-gems-release-1216-version-1-test-report.pdf (Ex. 3).

[17] *Dominion also handled 2009 NY congressional poll*, ABS-CBN News, May 7, 2010, https://news.abs-cbn.com/nation/05/07/10/dominion-also-handled-2009-ny-congressional-poll.

[18] Ina Reformina, *Source code firm Dominion sheds light on voting glitch*, ABS-CBN News, May 7, 2010, https://news.abs-cbn.com/nation/05/07/10/source-code-firm-dominion-sheds-light-voting-glitch.

[19] *See, e.g., Notice of Contract: Contract No. 071B7700117*, State of Michigan Enterprise Procurement: Department of Technology, Management, and Budget, 48 (2017), https://www.michigan.gov/documents/sos/071B7700117_Dominion_555356_7.pdf.

E. A Federal Judge in Georgia finds Dominion's voting systems are highly vulnerable to malicious manipulation.

38. Following the 2016 general election, a left-leaning advocacy organization and individual voters filed an action in the United States District Court for the Northern District of Georgia, seeking to set aside the results of a 2016 Congressional race in which the Republican candidate had prevailed. The *Curling v. Raffensperger* plaintiffs alleged "sophisticated hackers – whether Russian or otherwise – had the capability and intent to manipulate elections in the United States."[20] They later asked the court to enter a preliminary injunction barring Georgia in the 2020 general election from using Dominion's ballot marking devices from its Democracy Suite 5.5-A voting system. *See Curling v. Raffensperger*, No. 1:17-CV-2989-AT, 2020 WL 5994029, at *1 (N.D. Ga. Oct. 11, 2020).

39. On October 11, 2020, just three weeks before the 2020 general election, Judge Amy Totenberg[21] issued an order regarding the Dominion voting system's security risks and the potential for fraud or irregularities.[22] Judge Totenberg found substantial evidence that the Dominion system was plagued by security risks and the potential for votes to be improperly rejected or misallocated. She wrote, "The Plaintiffs' national security experts convincingly present evidence that this is not a question of 'might this actually ever

[20] Amended Complaint, Doc. 15, N.D. Ga. No. 2017CV292233 (Ex. 4).
[21] Given the hyper-partisan nature of the allegations and assertions set forth in Dominion's Complaint, it is worth noting that Judge Totenberg was nominated to the federal bench by President Obama in January of 2011.
[22] *Curling v. Raffensperger*, No. 1:17-CV-2989-AT, Doc. 964, 2020 WL 5994029, at *1 (N.D. Ga. Oct. 11, 2020) (Ex. 5).

happen?' – but 'when it will happen,' especially if further protective measures are not taken."[23]

40. Judge Totenberg's findings reflected many of the same issues which had existed more than ten years earlier with Diebold's system, ultimately purchased by Dominion:

- "[H]uge volume of significant evidence regarding the security risks and deficits in the [Dominion] system as implemented . . ."
- "Evidence presented in this case overall indicates the possibility generally of hacking or malware attacks occurring in voting systems and this particular system through a variety of routes – whether through physical access and use of a USB flash drive or another form of mini-computer, or connection with the internet."
- "[E]vidence credibly explaining how malware can mask itself when inserted in voting software systems or QR codes, erase the malware's tracks, alter data, or create system disruption."
- "Defendants [including Dominion] do not appear to actually dispute that cybersecurity risks are significant in the electoral sphere."
- Dominion's Director of Product Strategy and Security "acknowledged the potential for compromise of the [Dominion] operating system, by exploiting a vulnerability, that could allow a hacker to take over the Voting machine and compromise the security of the voting system software."
- "[F]ormidable amount of evidence that casts serious doubt on the validity of the use of the [risk-limiting audit statistical method for auditing election outcomes] with the current [Dominion] system."[24]

[23] *Id*. at *58 (Ex. 5 at 146).
[24] *Id*. at *10-12, 13, 14, 16, 17, 32, 35, 12, 57, 145, 146.

41. Judge Totenberg declined to enter a preliminary injunction because she felt bound by Eleventh Circuit precedent, and there was not enough time before the election to implement the requested relief—switching to paper ballots. Yet she expressed profound concern regarding the Dominion voting system, and Dominion's less than transparent actions:

> The Court's Order has delved deep into the true risks posed by the new [Dominion] voting system as well as its manner of implementation. These risks are neither hypothetical nor remote under the current circumstances. The insularity of the Defendants' and Dominion's stance here in evaluation and management of the security and vulnerability of the BMD system does not benefit the public or citizens' confident exercise of the franchise. The stealth vote alteration or operational interference risks posed by malware that can be effectively invisible to detection, whether intentionally seeded or not, are high once implanted.
>
> The Plaintiffs' national cybersecurity experts convincingly present evidence that this is not a question of 'might this actually ever happen?' — but 'when it will happen,' especially if further protective measures are not taken. Given the masking nature of malware and the current systems described here, if the State and Dominion simply stand by and say, "we have never seen it," the future does not bode well. [25]

42. Importantly, there is not a single case where a court has ruled on the merits of Dominion's voting machine integrity after having had a *full opportunity* to review the evidence. The *Curling* decision comes the closest to a review of Dominion.

F. Democratic lawmakers identify problems with Dominion's voting systems.

43. Within a year prior to the 2020 election, on December 6, 2019, four Democratic Members of Congress—Senator Elizabeth Warren, Senator Amy Klobuchar, Senator Ron Wyden, and Congressman Mark Pocan—published an open letter concerning

[25] *Id*. at *58 (Ex. 5 at 146).

major voting system manufacturers, including Dominion.[26] In the letter, they identified numerous problems:

- "trouble-plagued companies" responsible for manufacturing and maintaining voting machines and other election administration equipment, "have long skimped on security in favor of convenience," leaving voting systems across the country "prone to security problems."

- "the election technology industry has become highly concentrated ... Today, three large vendors – Election Systems & Software, Dominion, and Hart InterCivic – collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States."

- "Election security experts have noted for years that our nation's election systems and infrastructure are under serious threat. . . . voting machines are reportedly falling apart, across the country, as vendors neglect to innovate and improve important voting systems, putting our elections at avoidable and increased risk. . . . Moreover, even when state and local officials work on replacing antiquated machines, many continue to 'run on old software that will soon be outdated and more vulnerable to hackers.'"

- "[J]urisdictions are often caught in expensive agreements in which the same vendor both sells or leases, and repairs and maintains voting systems-leaving local officials dependent on the vendor, and the vendor with little incentive to substantially overhaul and improve its products.[]"[27]

44. Senator Warren, on her website, identifies an additional problem: "These vendors make little to no information publicly available on how much money they dedicate to research and development, or to maintenance of their voting systems and technology.

[26] Letter from Senators Warren, Klobuchar, and Wyden and Congressman Pocan to Steve D. Owens and Hootan Yaghoobzadeh (Dec. 6, 2019) (Ex. 6).
[27] *Id.*

They also share little or no information regarding annual profits or executive compensation for their owners."[28]

45. In August 2018, Senator Klobuchar stated on nationally broadcast television, Meet the Press, "I'm very concerned you could have a hack that finally went through. You have 21 states that were hacked into, they didn't find out about it for a year."[29]

46. Senator Wyden, also in the lead up to the 2020 election, explained during an interview, "[T]oday, you can have a voting machine with an open connection to the internet, which is the equivalent of stashing American ballots in the Kremlin. . . . [As] of today, what we see in terms of foreign interference in 2020 is going to make 2016 look like small potatoes. This is a national security issue! . . . The total lack of cybersecurity standards is especially troubling . . . But the lack of cybersecurity standards leads local officials to unwittingly buy overpriced, insecure junk. Insecure junk guarantees three things: a big payday for the election-tech companies, long lines on Election Day, and other hostile foreign governments can influence the outcome of elections through hacks."[30]

---

[28] *Warren, Klobuchar, Wyden, and Pocan Investigate Vulnerabilities and Shortcomings of Election Technology Industry with Ties to Private Equity*, Elizabeth Warren: United States Senator for MA (Dec. 10, 2019), https://www.warren.senate.gov/oversight/letters/warren-klobuchar-wyden-and-pocan-investigate-vulnerabilities-and-shortcomings-of-election-technology-industry-with-ties-to-private-equity.

[29] NBC News, Amy Klobuchar: Concerned That A 2018 Election Hack Could Succeed (Full) | Meet The Press | NBC News, YouTube (Aug. 5, 2018), https://www.youtube.com/watch?v=9wtUxqqLh6U.

[30] Mark Sullivan, *Senator Ron Wyden: The GOP is 'making a mockery' of election security*, FAST COMPANY (Feb. 19, 2020), available at https://www.fastcompany.com/90465001/senator-ron-wyden-the-gop-is-making-a-mockery-of-election-security.

G. After a thorough audit review, Dominion's systems fail to obtain certification.

47. On October 2-3, 2019, Dominion presented its Democracy Suite 5.5-A voting system in Texas for examination and certification.[31] It failed the test.

48. "The examiner reports identified multiple hardware and software issues . . . Specifically, the examiner reports raise concerns about whether the Democracy Suite 5.5-A system is suitable for its intended purpose; operates efficiently and accurately; and is safe from fraudulent or unauthorized manipulation.[32]

49. On January 24, 2020, the Texas Secretary of State denied certification of the system for use in Texas elections. Texas's designated experts who evaluated Democracy Suite 5.5-A flagged risk from the system's connectivity to the internet despite "vendor claims" that the system is "protected by hardening of data and IP address features."[33, 34] "[T]he machines could be vulnerable to a rogue operator on a machine if the election LAN is not confined to just the machines used for the election . . . The ethernet port is active on the ICX BMD during an election. . . . This is an unnecessary open port during the voting period and could be used as an attack vector."[35] Other security vulnerabilities found by Texas include use of a "rack mounted server" which "would typically be in a room other

---

[31] Jose A. Esparza, *Report of Review of Dominion Voting Systems Democracy Suite 5.5A*, Tex. Sec'y of State (Jan. 24, 2020), available at https://www.sos.texas.gov/elections/forms/sysexam/dominion-d-suite-5.5-a.pdf (Ex. 7).
[32] *Id.*
[33] Letter from Brandon Hurley to Keith Ingram (Feb. 19, 2019) (Ex. 8).
[34] James Sneeringer, Ph.D., *Voting System Examination: Dominion Voting Systems Democracy Suite 5.5-A* 2, 5 (TX Sec. of State Elections Div.), available at https://www.sos.texas.gov/elections/forms/sysexam/oct2019-sneeringer.pdf.
[35] Tom Watson, *Democracy Suite 5.5A* 4-5 (TX Sec. of State Elections Div.), available at https://www.sos.texas.gov/elections/forms/sysexam/oct2019-watson.pdf.

than a room used for the central count" and would present a security risk "since it is out of sight."[36]

50. Texas Attorney General Ken Paxton later explained, "We have not approved these voting systems based on repeated software and hardware issues. It was determined they were not accurate and that they failed — they had a vulnerability to fraud and unauthorized manipulation."[37]

H. Media reports and government findings expose longstanding, fundamental vulnerabilities in electronic voting systems.

51. Election officials and voting system manufacturers, including Dominion's CEO, have publicly denied that voting machines are connected to the internet and, therefore, not susceptible to attack via the internet.[38] Dominion's CEO, John Poulos, testified in December 2020 that Dominion's voting systems are "closed systems that are not networked meaning they **are not connected to the internet**." This is false.

52. Vice reported in 2019, "[A] group of election security experts have found what they believe to be nearly three dozen backend election systems in 10 states connected to the internet over the last year, including some in critical swing states. These include systems in nine Wisconsin counties, in four Michigan counties, and in seven Florida

---

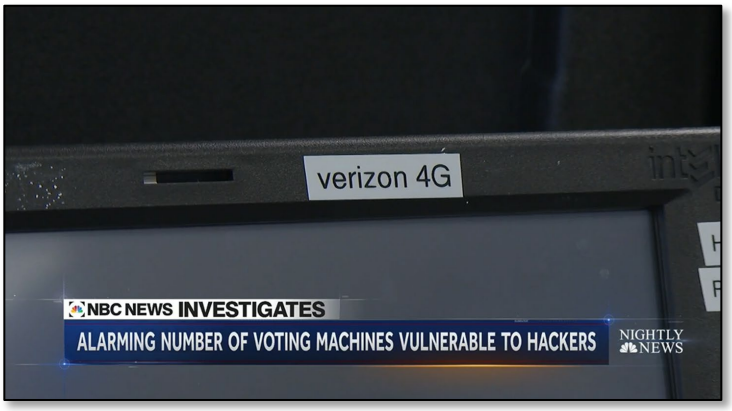
[36] *Id.*

[37] Brad Johnson, *Texas Rejected Use of Dominion Voting System Software Due to Efficiency Issues*, The Texan, Nov. 19, 2020, https://thetexan.news/texas-rejected-use-of-dominion-voting-system-software-due-to-efficiency-issues/.

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

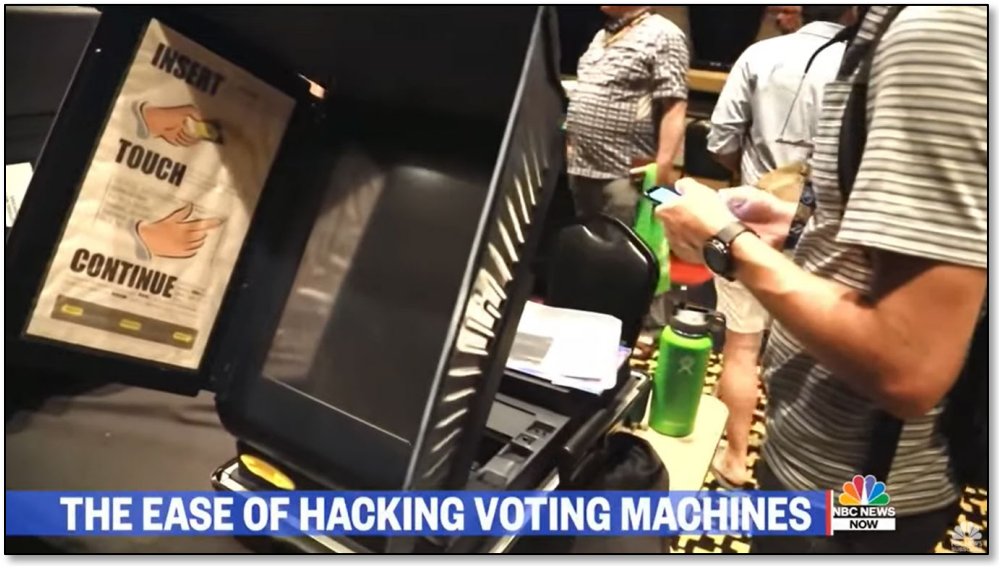
counties. . . . [A]t least some jurisdictions were not aware that their systems were online[.] . . . Election officials were publicly saying that their systems were never connected to the internet because they didn't know differently."[39] In 2020, a team of election security experts found more than 35 voting systems were online.[40]

53. In 2020, NBC reported that voting machines were in fact connected to the internet, making them susceptible to hacking, and "The three largest voting manufacturing companies — Election Systems & Software, Dominion Voting Systems and Hart InterCivic — have acknowledged they all put modems in some of their tabulators and scanners. . . . Those modems connect to cell phone networks, which, in turn, are connected to the internet . . . . 'Once a hacker starts talking to the voting machine through the modem . . . they can hack the software in the voting machine and make it cheat in future elections,' [a Princeton computer science professor and expert on elections] said."[41]



[39] *Id.*
[40] Kevin Monahan, Cynthia McFadden, and Didi Martinez, 'Online and Vulnerable': Experts find nearly three dozen U.S. voting systems connected to internet, NBC News, Jan. 10, 2020, available at https://www.nbcnews.com/politics/elections/online-vulnerable-experts-find-nearly-three-dozen-u-s-voting-n1112436.
[41] *Id.*

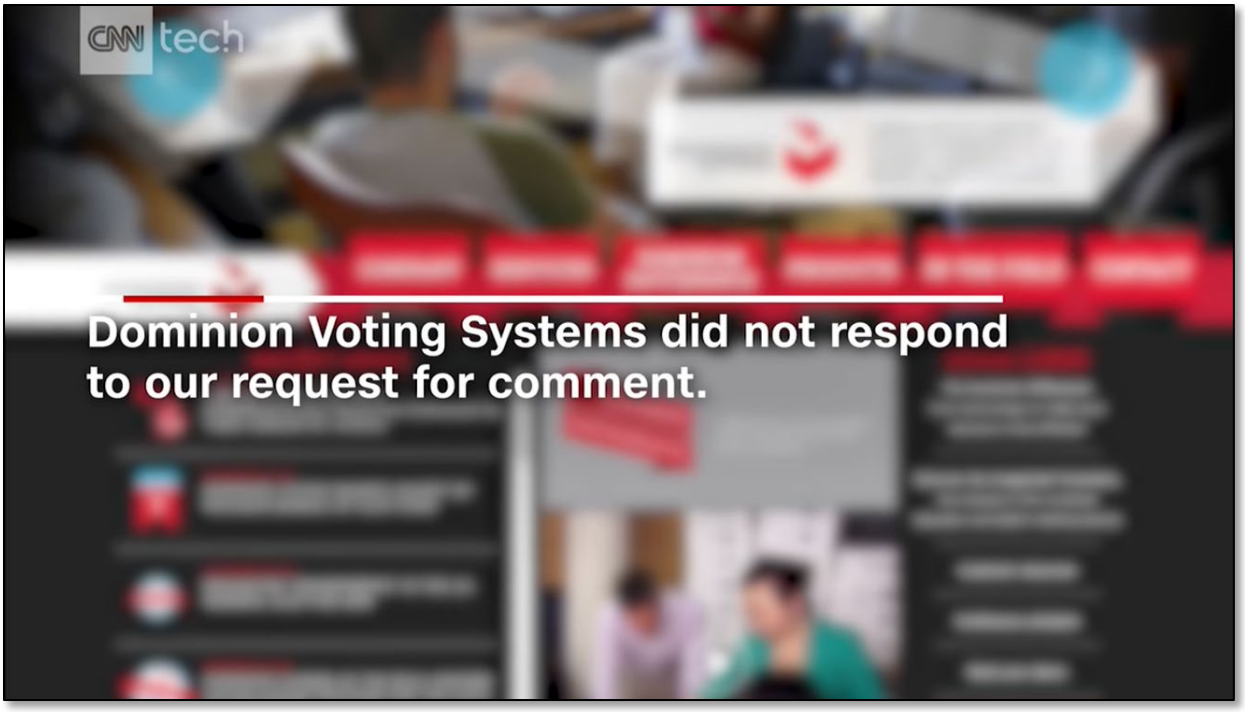
54. In a 2019 story about the DEF CON hacking conference, NBC News reported that Dominion avoided participation in the conference; that hackers can target voting systems with ease; and that Dominion's voting machines are connected to the internet.[42]



55. In 2017, Dominion refused to respond to CNNTech's request for comment about its hackable voting machines.[43] CNNTech also asked Jake Braun, a former security advisor for the Obama administration and organizer of the DEF CON hacking conference, "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. . . ."[44]

---

[42] NBC News, *How Hackers Can Target Voting Machines | NBC News Now*, YouTube (Aug. 12, 2019), https://www.youtube.com/watch?v=QtWP0KDx2hA.
[43] CNN Business, *We watched hackers break into voting machines*, YouTube (Aug. 11, 2017), https://www.youtube.com/watch?v=HA2DWMHgLnc.
[44] *Id.*



56. The Congressional Task Force on Election Security's Final Report in January 2018 identified the vulnerability of U.S. elections to foreign interference:[45] "According to DHS, Russian agents targeted election systems in at least 21 states, stealing personal voter records and positioning themselves to carry out future attacks. . . media also reported that the Russians accessed at least one U.S. voting software supplier . . . in most of the targeted states officials saw only preparations for hacking . . . [but] in Arizona and Illinois, voter registration databases were reportedly breached. . . If 2016 was all about preparation, what more can they do and when will they strike? . . . [W]hen asked in March about the prospects for future interference by Russia, then-FBI Director James Comey testified before Congress that: "[T]hey'll be back. They'll be back in 2020. They may be back in 2018."[46]

[45] CONGRESSIONAL TASK FORCE ON ELECTION SECURITY, FINAL REPORT (2018) (Ex. 9).
[46] *Id*. at 6-7.

57. The Congressional Task Force on Election Security report also stated that "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."[47]

58. In 2016, "Russian agents probed voting systems in all 50 states, and successfully breached the voter registration systems of Arizona and Illinois."[48] The Robert Mueller report and a previous indictment of twelve Russian agents 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."[49]

59. A 2015 report issued by the Brennan Center for Justice listed two and a half-pages of instances of issues with voting machines, including a 2014 post-election investigation into machine crashes in Virginia which found "voters in Virginia Beach observed that when they selected one candidate, the machine would register their selection

---

[47] *Id*. at 25 (citing Matt Blaze, *et al*., *DEFCON 25 Voting Machine Hacking Village: Rep. on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, 16 (2017) available at https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf).

[48] 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.

[49] Report On The Investigation Into Russian Interference In The 2016 Presidential Election, p. 50, available at https://www.justice.gov/archives/sco/file/1373816/download.

for a different candidate."[50] The investigation also found that the Advanced Voting Solutions WINVote machine, which is Wi-Fi-enabled, "had serious security vulnerabilities" because wireless cards on the system could allow "an external party to access the [machine] and modify the data [on the machine] without notice from a nearby location," and "an attacker could join the wireless ad-hoc network, record voting data or inject malicious [data.]"[51]

60. HBO's documentary *Kill Chain: The Cyber War on America's Elections*,[52] details the vulnerability of election voting machines, including Dominion's. Harri Hursti, a world-renowned data security expert, showed that he hacked digital voting machines to *change votes* in 2005. According to Hursti, the same Dominion machine that Mr. Hursti hacked in 2005 was slated for use in 20 states for the 2020 election.

61. In the documentary, Marilyn Marks, Executive Director of Coalition of Good Governance (one of the Plaintiffs in *Curling*), stated, "In Georgia, we ended up seeing the strangest thing. In a heavily Democratic precinct, there was one machine out of a seven-machine precinct that showed heavy Republican wins, while the precinct itself and all of the other machines were showing heavy Democratic wins." Dr. Kellie Ottoboni,

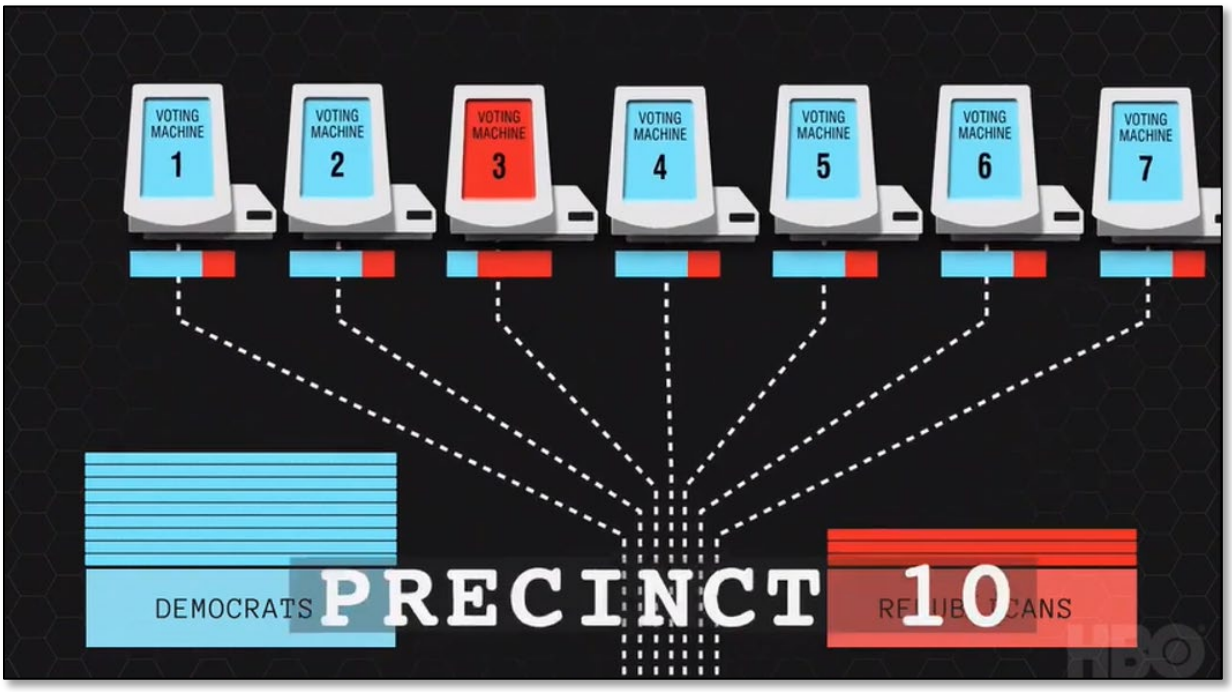
---

[50] Lawrence Norden and Christopher Famighetti, *AMERICA'S VOTING MACHINES AT RISK*, Brennan Ctr. for Just., 13 (Sep. 15, 2014), available at https://www.brennancenter.org/sites/default/files/2019-08/Report_Americas_Voting_Machines_At_Risk.pdf (Ex. 10).

[51] *Id.*

[52] Simon Ardizzone, Russell Michaels, and Sarah Teale, *Kill Chain: The Cyber War on America's Elections*, HBO (Mar. 26, 2020), available at https://play.hbomax.com/feature/urn:hbo:feature:GXk7d3QAJHI7CZgEAACa0?reentered=true&userProfileType=liteUserProfile.

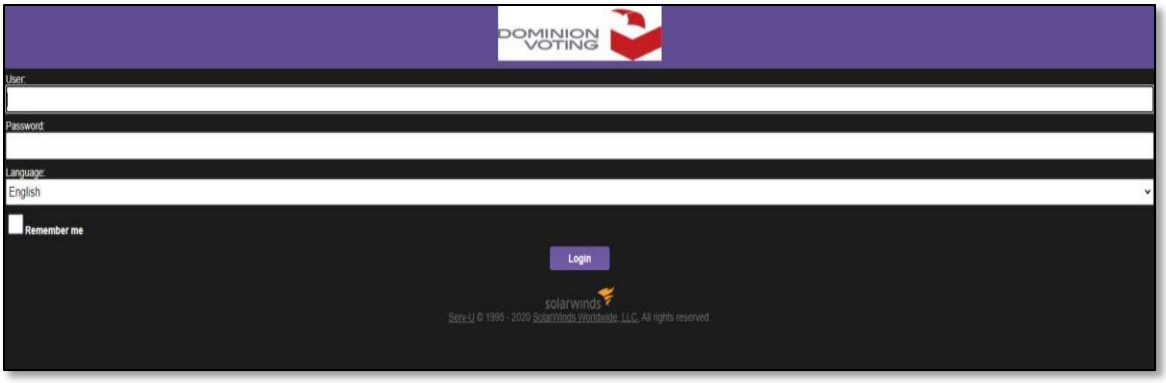
Department of Statistics, UC Berkeley, stated the likelihood of this happening is "an astronomically small chance." It was less than one in a million.[53]



62. In December 2020, the Department of Homeland Security's Cybersecurity & Infrastructure Agency ("CISA") revealed that hackers infiltrated SolarWinds software.[54] Despite CEO Poulos's claim that Dominion had never used SolarWinds, an archival screenshot of Dominion's website shows a now-erased SolarWinds logo (screenshot below). Dominion in fact did use SolarWinds.

[53] Screenshot from https://www.facebook.com/KillChainDoc/videos/2715244992032273/.

[54] Zachary Stieber, *Dominion Voting Systems Uses Firm That Was Hacked*, THE EPOCH TIMES, Dec. 14, 2020, https://www.theepochtimes.com/mkt_app/dominion-voting-systems-uses-firm-that-was-hacked_3617507.html.



63. Dominion refuses to provide access to experts to forensically investigate its "proprietary" software, machines, and systems, to further establish that its machines have been hacked. This is telling in and of itself. Dominion denies the public access to the evidence to substantiate that it has been hacked. It silences anyone who makes this claim while simultaneously denying access to the key information one way or the other.

I. Evidence shows that Dominion's voting machines were manipulated during the 2020 elections.

64. On Monday, November 2, 2020, the night before the 2020 election, Dominion forced unplanned and unannounced software uploads into its machines. In some counties in Georgia, Dominion's irregular software update caused voting machines to crash the next day during the election. The supervisor of one County Board of Elections stated that Dominion "uploaded something last night, which is not normal, and it caused a glitch," and "[t]hat is something that they don't ever do. I've never seen them update anything the day before the election."[55]

[55] Kim Zetter, *Cause of Election Day glitch in Georgia counties still unexplained*, POLITICO, Nov. 4, 2020, https://www.politico.com/news/2020/11/04/georgia-election-machine-glitch-434065.

65. During the 2020 election Dominion machines across the country were connected to the internet when they should not have been. A Dominion representative assigned to Wayne County, Michigan reported numerous irregularities with the election process and Dominion's machines, including that the voting machines were connected to the internet and that the machines had scanning issues. In Wisconsin, Dominion machines that were not supposed to be connected to the internet were in fact connected to a "hidden" Wi-Fi network during voting.[56]

66. Attorneys representing a Democratic candidate who lost in 2020 filed a brief raising Dominion machine errors and election issues, arguing, "discrepancies between the number of votes cast and the number of votes tabulated have been pervasive in the counting of ballots for this race . . . In addition to the table-to-machine count discrepancies of which the parties are aware, there have also been procedural inconsistencies that question the integrity of the process . . . [T]he audit results revealed 'unexplained discrepancies' but failed to provide any explanation . . . what caused those discrepancies or if they were ever resolved . . . In this case, there is reason to believe that voting tabulation machines misread *hundreds* if not *thousands* of valid votes as undervotes . . ."[57]

67. Michael Spitzer-Rubenstein, a political operative, was given internet access to a hidden Wi-Fi network at an election center where votes were being counted.[58] Spitzer-

---

[56] M.D. Kittle, *EMAILS: GREEN BAY'S 'HIDDEN' ELECTION NETWORKS*, WISCONSIN SPOTLIGHT, Mar. 21, 2021, https://wisconsinspotlight.com/emails-green-bays-hidden-election-networks/.

[57] Oswego County, Index No. ECF 2020-1376, dated February 1, 2021 at 2.

[58] M.D. Kittle, *Democrats' Operative Got Secret Internet Connection at Wisconsin Election Center, Emails Show*, DAILY SIGNAL, Mar. 23, 2021, available at

Rubenstein received an email from Trent James, director of event technology at Green Bay's Central Count location, which stated, "One SSID [for a Wi-Fi network] will be hidden and it's: 2020vote. There will be no passwords or splash page for this one and it should only be used for the sensitive machines that need to be connected to the internet." Four other individuals were copied on the email.

68. Following the 2020 election, state lawmakers initiated investigations and audits of the results, often directing particular attention to Dominion's voting systems.

a. Congressman Paul Gosar called for a special session of the Arizona legislature to investigate the accuracy and reliability of the Dominion ballot software.[59] On January 27, 2021, the Maricopa County, Arizona Board of Supervisors voted unanimously to approve an audit of the 2020 election results and a forensic audit of Dominion's voting machines.[60] The Arizona senate hired a team of forensic auditors consisting of four companies to review Maricopa's election process.[61] A week later, attorneys sent each of those four companies a threatening cease-and-desist letter, improperly

https://www.dailysignal.com/2021/03/23/democrats-operative-got-secret-internet-connection-at-wisconsin-election-center-emails-show/.

[59] Hannah Bleau, *Rep. Paul Gosar Calls on Arizona Officials to 'Investigate the Accuracy' of the Dominion Ballot Software After Reports of 'Glitches,'* BREITBART, Nov. 7, 2020, https://www.breitbart.com/politics/2020/11/07/rep-gosar-calls-on-az-officials-investigate-the-accuracy-of-the-dominion-ballot-software-after-reports-of-glitches/.

[60] AUDITING ELECTIONS EQUIPMENT IN MARICOPA COUNTY, https://www.maricopa.gov/5681/Elections-Equipment-Audit (last visited Apr. 18, 2021).

[61] Press Release, Arizona State Senate, Arizona Senate hires auditor to review 2020 election in Maricopa County (Mar. 31, 2021) (on file with author) (Ex. 11).

attempting to influence the reviews.[62] The audit is scheduled for April 19 to May 14, 2021.

b. In the Michigan case of *Bailey v. Antrim*, Cyber Ninjas and CyFir have found Dominion voting machines are connected to the internet, either by Wi-Fi or a LAN wire; there are multiple ways election results could be modified and leave no trace; and the same problems have been around for 10 years or more.[63]

c. On April 12, 2021, New Hampshire Governor Christopher Sununu announced he had signed legislation appointing an audit of a Rockingham County race which relied upon Dominion voting machines after suspicious uniform shorting of vote tallies for four candidates was uncovered.

d. On March 23, 2020 the Wisconsin Assembly ordered an investigation into the 2020 election. Wisconsin uses Dominion voting machines.[64]

e. Investigations into election irregularities are also ongoing in Pennsylvania and Georgia, states which also use Dominion voting machines.

69. Even the Biden administration has recently sanctioned Russia for election interference and hacking.

---

[62] Letter from Sara Chimene-Weiss, James E. Barton II, Roopali H. Desai, and Sarah R. Gonski to Cyber Ninjas, CyFir, Digital Discovery, and Wake Technology Services (Apr. 6, 2021) (Ex. 12).

[63] Pl.'s Collective Resp. to Defs.' and Non-Party Counties' Mots. to Quash and for Protective Orders at Exs. 7-8 (April 9, 2021), Bailey v. Antrim County (No. 20-9238).

[64] Scott Bauer, *Wisconsin Assembly OKs investigation into 2020 election*, FOX6 NEWS MILWAUKEE, Mar. 23, 2020, https://www.fox6now.com/news/wisconsin-assembly-approves-election-investigation.

J. Dominion is using the legal process to censor, attack, and destroy anyone who questions the 2020 election and voting machine hacking and manipulation.

70. Through aggressive litigation, threats of litigation, and publicization of these activities, Dominion seeks to stop criticism of election voting machines and suppress information about how its machines have been hacked in American elections. This campaign of "lawfare" is intended to stifle *any* and *all* public debate about the reliability of the election results, whether such speech is related to Dominion or not.

71. Dominion has filed a $1.3 billion lawsuit against Sidney Powell. Dominion has filed a $1.3 billion lawsuit against Rudy Giuliani. Dominion has filed a $1.6 billion lawsuit against Fox News. Dominion has filed a $1.3 billion lawsuit against MyPillow and its CEO. Yet Dominion's annual revenues are only about $90 million.[65] Dominion's exaggerated lawsuits are not about any damages it has suffered; they are designed to intimidate those who exercise their right to free speech about the election.

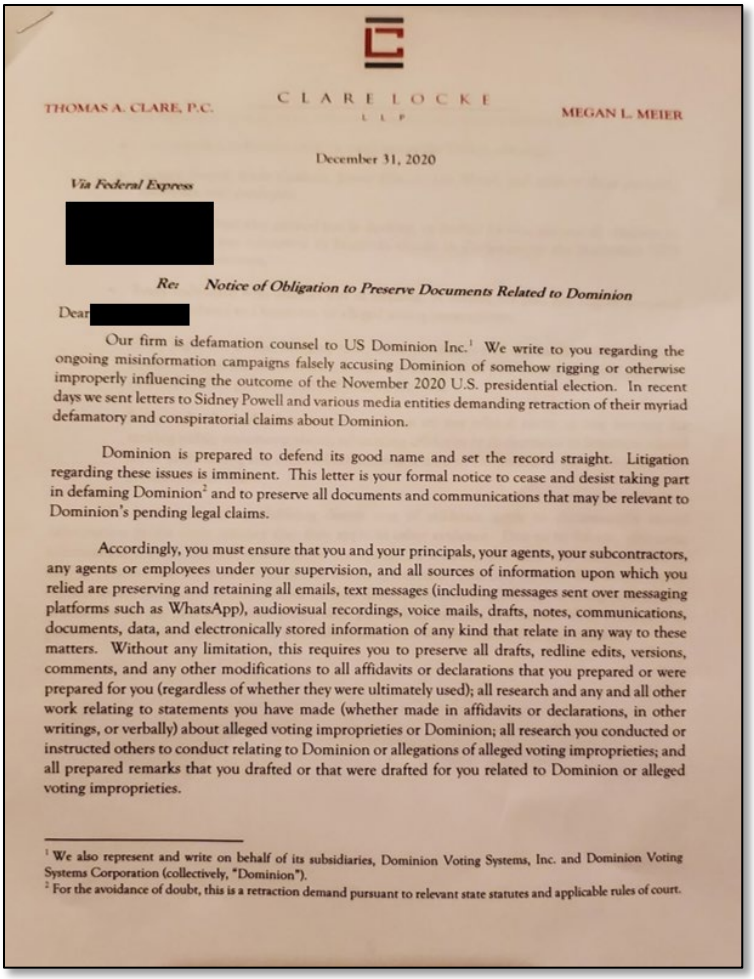
72. Dominion amplifies the effect of its exaggerated lawsuits with threatening letters and a publicity campaign.

a. Dominion has sent at least 150 attorney letters, threatening the recipients with legal action. Some of these letters include copies of Dominion's legal papers in its lawsuits. The clear message of these letters is that anyone who comments publicly about Dominion will be ruined.

[65] "The entire sector generates only about $300 million in revenue annually, according to Harvard professor Stephen Ansolabehere, who studies elections and formerly directed the Caltech/MIT Voting Technology Project," and "Dominion, [] has about 30% of the market." https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it.

b. Dominion sent threatening letters to numerous individuals who signed sworn affidavits that were used in litigation about the election process. In many cases, the poll watchers' affidavits did not include any statement about Dominion or the election. But Dominion's campaign is total; it seeks to deter *any public expression* about the election. Dominion's clear threats that it will sue witnesses who testify about election irregularities or fraud does not threaten just the individual witnesses; it threatens the integrity of the justice system as a whole.

c. In one instance, Dominion sent an intimidating letter to *the uncle* of an attorney involved in litigation about the 2020 election. The uncle himself had no involvement, but for the circumstance of being related to someone investigating Dominion and the election, Dominion accused him of disseminating misinformation and making false accusations. Its letter threatened, "Litigation regarding these issues is imminent."



CLARE LOCKE LLP

THOMAS A. CLARE, P.C. MEGAN L. MEIER

December 31, 2020

Via Federal Express

[redacted]

Re: Notice of Obligation to Preserve Documents Related to Dominion

Dear [redacted]

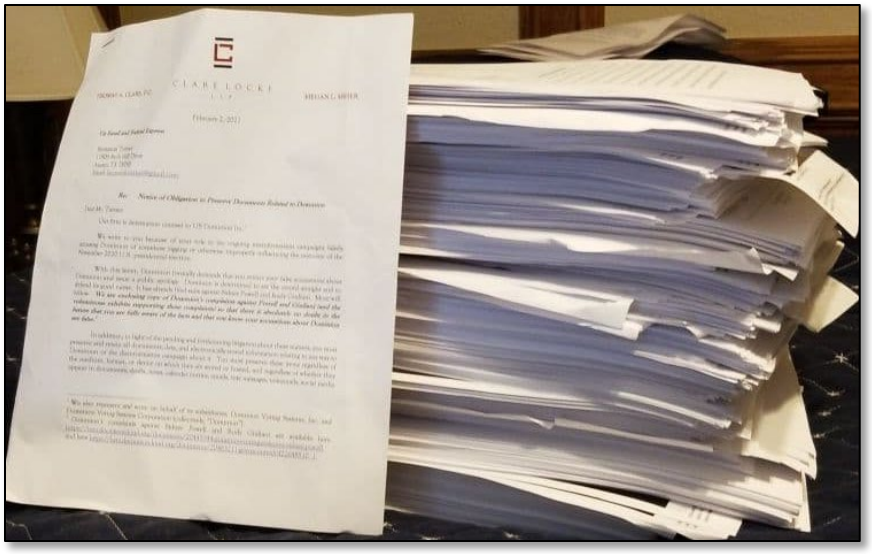
Our firm is defamation counsel to US Dominion Inc.[1] We write to you regarding the ongoing misinformation campaigns falsely accusing Dominion of somehow rigging or otherwise improperly influencing the outcome of the November 2020 U.S. presidential election. In recent days we sent letters to Sidney Powell and various media entities demanding retraction of their myriad defamatory and conspiratorial claims about Dominion.

Dominion is prepared to defend its good name and set the record straight. Litigation regarding these issues is imminent. This letter is your formal notice to cease and desist taking part in defaming Dominion[2] and to preserve all documents and communications that may be relevant to Dominion's pending legal claims.

Accordingly, you must ensure that you and your principals, your agents, your subcontractors, any agents or employees under your supervision, and all sources of information upon which you relied are preserving and retaining all emails, text messages (including messages sent over messaging platforms such as WhatsApp), audiovisual recordings, voice mails, drafts, notes, communications, documents, data, and electronically stored information of any kind that relate in any way to these matters. Without any limitation, this requires you to preserve all drafts, redline edits, versions, comments, and any other modifications to all affidavits or declarations that you prepared or were prepared for you (regardless of whether they were ultimately used); all research and any and all other work relating to statements you have made (whether made in affidavits or declarations, in other writings, or verbally) about alleged voting improprieties or Dominion; all research you conducted or instructed others to conduct relating to Dominion or allegations of alleged voting improprieties; and all prepared remarks that you drafted or that were drafted for you related to Dominion or alleged voting improprieties.

[1] We also represent and write on behalf of its subsidiaries, Dominion Voting Systems, Inc. and Dominion Voting Systems Corporation (collectively, "Dominion").
[2] For the avoidance of doubt, this is a retraction demand pursuant to relevant state statutes and applicable rules of court.

d. Another individual, an actuary, performed statistical analyses, inquiring whether the presence of Dominion voting machines affected election outcomes. He found nonrandom differences in counties that used Dominion machines. Dominion mailed him a box, pictured below, full of legal papers, which included lawsuits filed against other citizens along with a threatening demand letter. As a result of speaking out, the actuary lost business and was forced to self-censor.



73. To further amplify the impact of its legal letters and exaggerated lawsuits, Dominion has bragged about and widely publicized them, seeking to ensure that everyone – not just the recipients of its attorney letters – knows they will be punished if they speak against Dominion, and anyone could be the next victim of a Dominion billion-dollar lawsuit. For example:

a. In a nationally televised interview, Dominion CEO John Poulos announced, **"Our legal team is looking at frankly everyone, and we're not ruling anybody out."** He said Dominion's previous lawsuit was "definitely not the last lawsuit" it would be filing.

b. Dominion's website prominently displays its lawsuits, even ahead of its own products, and statements from its attorneys. The website boasts, "Dominion has sent preservation request letters to Powell, Giuliani, Fox, OAN, and Newsmax, as well as more than 150 other individuals and news organizations. Stay tuned to this page for updates."

74. The substantial expense of litigation in defamation lawsuits brought by governmental actors (like Dominion) against their critics has an enormous chilling effect on speech. Dominion has issued a general threat to all ("Our legal team is looking at frankly everyone, and we're not ruling anybody out") and sharpened that threat by delivering it to specific individuals ("litigation regarding these issues is imminent") – sometimes accompanied by copies of lawsuits Dominion had already filed against others.

75. Dominion's use of lawfare tears at the fabric of our constitutional order. If successful, the scheme will cripple our system's ability to ferret out and stop electoral manipulation, as well as cut a wide hole in the First Amendment.

K. Mike Lindell Speaks out about the 2020 elections.

76. Mike Lindell, the CEO of MyPillow, has spoken out in his personal capacity about Dominion, about electronic voting machines, and on issues of election integrity. Lindell made speeches, gave interviews, and posted his thoughts and opinions on social media.

77. In making these statements, Lindell spoke for himself, not MyPillow. MyPillow has not engaged in discussion about the 2020 election. However, as an American company supporting American constitutional values, MyPillow unreservedly supports Lindell's right to exercise his First Amendment freedoms concerning the matters of critical public concern, like election matters.

L. Dominion attacks Lindell and MyPillow.

78. Dominion aggressively pushed a narrative that there should be no concern regarding the integrity of the election. Dominion took equally aggressive action to demand no criticism. In response to Lindell's exercise of his First Amendment free speech rights, Dominion launched its lawfare campaign against both Lindell and MyPillow. Lawfare is the use of the legal system as part of wrongful scheme to attack another person and inflict extra-judicial harm upon them. Here, Dominion's scheme is wrongful because Dominion's purpose is to punish and deter important constitutionally-protected activity–free expression about a matter of public concern.

79. In furtherance of this scheme, Dominion had threatening lawyer letters delivered, filed enormous lawsuits against MyPillow (and others), sensationalized the lawsuits through a large media campaign, and threatened to file additional lawsuits against

anyone who exercises their constitutionally protected right to free expression in a matter contrary to the interests of Dominion and its allies. Dominion has issued a general threat to all ("our legal team is looking at frankly everyone, and we're not ruling anybody out" and sharpened that threat by delivering it to specific individuals ("Litigation regarding these issues is imminent") – sometimes accompanied by copies of lawsuits Dominion already filed.

80. MyPillow and its employees have suffered severe extra-judicial harm from Dominion's scheme.

M. Dominion's wrongful attack against MyPillow and the damaging fallout.

81. Dominion's campaign descends from a long and sad history in this country, the McCarthy era in which lives and organizations were destroyed, and families torn apart, for being labeled a Communist. Just as during that era being *associated* with a suspected Communist could end a professional career,[66] so too today, those who, like MyPillow are merely associated with a critic of Dominion and the integrity of the 2020 election, face expulsion from public life in large parts of America. Dominion is using today's cancel culture to eliminate dissent and to cover up the election issues that compromised the 2020 result.

82. Even giant, publicly traded retailers are not immune from public opinion and political pressures. Fearing retribution in the marketplace, many of MyPillow's

[66] James E. Moliterno, *Politically Motivated Bar Discipline*, 83 WASH. U. L. Q., 725, 729 (2005).

commercial suppliers and buyers have as a direct result of Dominion's crusade terminated longstanding relationships with MyPillow which were projected to grow.

a. Directly following Dominion's publicized threats to sue MyPillow's CEO, as promoted through national media, a nationwide retailer canceled a significant purchase order with MyPillow.

b. Directly following Dominion's filing of its lawsuit against MyPillow, MyPillow lost another significant nationwide-retailer customer.

c. A third retailer cited the coverage in the media of Dominion's campaign as the reason for cutting ties with MyPillow.

d. Numerous others have cut ties as well, for the same reasons.[67]

83. MyPillow has suffered the loss of access to marketing media as a result of Dominion's highly publicized lawfare campaign.

a. Following Dominion's lawsuit against MyPillow, a radio station representing a key advertising stream canceled its relationship with MyPillow.

b. Many of MyPillow's social media platforms have been limited, restricted, or removed altogether. Immediately following, and as a direct result of Dominion's legal threats and media attacks against MyPillow, MyPillow

[67] Justin Barclay, *The Official List of Every Business That Has Dropped MyPillow*, WEST MICHIGAN LIVE BLOG (Feb. 10, 2021), https://woodradio.iheart.com/content/2021-02-10-the-official-list-of-every-business-that-has-dropped-mypillow/.

was deplatformed from a major social media outlet, which significantly harmed the company and the brand.

84. MyPillow has suffered from attacks on the employees on whom it relies to accomplish its production and sales.

a. MyPillow employees are subjected to daily hateful and barbaric calls, emails, and comments on the company's social media platforms.

b. MyPillow employees have been subjected to ridicule in their personal lives, and death threats necessitating protection from local law enforcement. Dominion's actions have seeped into nearly every aspect of their personal lives, including their ability to use social media freely and feel comfortable in their homes, neighborhoods, and workplace.

c. MyPillow employees have been forced to limit (and even remove) private social media posts, profile pictures, information, and accounts for fear of harassment by Dominion and those it stirs up.

85. All this damage to MyPillow and its employees was intentionally caused by Dominion. MyPillow has not made a single statement about Dominion prior to Dominion's lawsuit. Dominion nonetheless targeted MyPillow and its employees with one of the largest defamation lawsuits in history and encouraged a firestorm of media coverage in order to punish MyPillow for the free speech of its founder—and to send a message to others to stay silent.

86. MyPillow has never entered the public debate about the 2020 election; again, it has made no statement about Dominion whatsoever. Yet Dominion, an agent of the

government, has intentionally and wrongfully inflicted great harm upon MyPillow and its employees.

87. Resulting from Defendants' conduct, Plaintiff has suffered and is continuing to suffer damages, including but not limited to a reasonable multiple of enterprise value, exceeding $1.6 billion.

V. CAUSES OF ACTION

Count 1
42 U.S.C. § 1983
Free Speech – Violation of First and Fourteenth Amendments
(Lawfare)

88. MyPillow repeats and realleges all allegations set forth above as if they were stated in full and incorporated herein.

89. Defendants, at all times relevant hereto, were performing and fulfilling a traditional and exclusive state and governmental function of administering public elections, pursuant to state statutes, ordinances, regulations, customs, rules and policies established thereunder, and as such, were acting under color of state law.

90. As detailed above, Defendants, in their role as agents of the state administering public elections, have conducted an expansive illegal campaign which was designed to, and did, punish and silence any voice that criticized or questioned Defendants' actions or products.

91. Defendants' illegal campaign to punish and silence their critics violates the Free Speech Clause of the First Amendment as applied to the states and their political subdivisions and agents under the Fourteenth Amendment and 42 U.S.C. § 1983.

92. Defendants intended to harm Plaintiff as part of their illegal campaign because of Plaintiff's affiliation with its CEO Mike Lindell, who publicly expressed opinions that Defendants wrongfully sought to suppress and punish.

93. Defendants' illegal campaign to punish and silence their critics violated the protected speech rights of MyPillow, its executives, and its employees by (a) intentionally seeking, through threats, intimidation, and litigation, to deter MyPillow, its executives, and its employees from exercising their free speech rights, thereby chilling their future exercise of their Constitutional rights; and (b) intentionally seeking, through threats, intimidation, and litigation, to deter MyPillow from expressing in the future any idea or opinion disliked by Defendants in MyPillow's advertising and promotional materials, including the use of particular words as coupon codes.

94. Defendants' deprivation of MyPillow's and its executives' and employees' Constitutional rights, both directly and as third parties, caused injury to MyPillow, including, but not limited to, loss of long-standing business relationships, loss of customer and supplier contracts, loss of promotional access in media, expenditure of attorney fees, emotional distress of employees resulting from threats and verbal attacks, diversion of employee time and attention away from MyPillow, and the chilling of MyPillow's Constitutional right to free speech and expression.

95. Resulting from Defendants' conduct, Plaintiff has suffered damages as described herein.

Count 2
42 U.S.C. § 1983
Reprisal

96. MyPillow repeats and realleges all allegations set forth above as if they were stated in full and incorporated herein.

97. Defendants, at all times relevant hereto, were performing and fulfilling a traditional and exclusive state governmental function of administering public elections, pursuant to state statutes, ordinances, regulations, customs, rules and policies established thereunder, and as such, were acting under color of state law.

98. Defendants intended to harm Plaintiff as part of their illegal campaign, because of Plaintiff's affiliation with its CEO Mike Lindell, who publicly expressed opinions that Defendants wrongfully sought to suppress and punish.

99. Defendants' reprisal actions were motivated, at least in part, by MyPillow's and its CEO's exercise of their free speech rights protected under the First Amendment and, as applied against the states and their political subdivisions and agents, the Fourteenth Amendment.

100. Defendants' reprisal actions would chill a person of ordinary firmness from continuing in the constitutionally protected activity, and indeed, Defendants' reprisal actions have chilled MyPillow, its executives, and its employees from exercising their First Amendment free speech rights.

101. Defendants' deprivation of MyPillow's and its executives' and employees' Constitutional rights, both directly and as third parties, caused injury to MyPillow, including, but not limited to, loss of long-standing business relationships, loss of customer

and supplier contracts, loss of promotional access in media, expenditure of attorney fees, emotional distress of employees resulting from threats of verbal attacks, diversion of employee time and attention away from MyPillow, and the chilling of MyPillow's Constitutional right to free speech and expression.

102. Resulting from Defendants' conduct, Plaintiff has suffered damages as described herein.

Count 3
42 U.S.C. § 1983
Fourteenth Amendment Violations

103. MyPillow repeats and realleges all allegations set forth above as if they were stated in full and incorporated herein.

104. Defendants, at all times relevant hereto, were performing and fulfilling a traditional and exclusive state governmental function of administering public elections, pursuant to state statutes, ordinances, regulations, customs, rules and policies established thereunder, and as such, were acting under color of state law.

105. As detailed above, Defendants, in their role as agents administering public elections, have conducted an expansive illegal campaign which was designed to, and did, punish and silence any voice that criticized or questioned Defendants' actions or products – in part by creating public pressure on Plaintiff's commercial counterparties to terminate their relationships with Plaintiff.

106. Defendants intended to harm Plaintiff as part of their illegal campaign, because of Plaintiff's affiliation with its CEO Mike Lindell, who publicly expressed opinions that Defendants wrongfully sought to suppress and punish.

107. As the result of Defendants' actions, and as expected and intended by them, Plaintiff suffered the loss of substantial property interests, including, but not limited to, loss of long-standing business relationships, loss of supplier contracts, and loss of access to promotional access in media.

108. Plaintiff was not provided due process in connection with the loss of its property interests caused by Defendants.

109. In the alternative, Defendants illegally created a danger of injury to Plaintiff, and Plaintiff was then injured in its property interests through the danger source created by Defendants.

a. Plaintiff was a member of a limited, precisely definable group, specifically, individuals and entities targeted by Defendants on the basis of their expression of ideas that Defendants desired to suppress or their affiliation with someone who expressed ideas that Defendants desired to suppress.

b. Defendants' conduct put Plaintiff at a significant risk of serious, immediate and proximate harm. Specifically, Defendants' campaign of threats, litigation, and public vilification created, and was intended to create, a significant risk that contract partners, suppliers, media sources, and others in the marketplace would terminate Plaintiff's supply relationships, sales channels, and marketing avenues. Defendants sought to, and did, stir up the ostracization and termination of Plaintiff from its commercial connections.

c. The risk of this outcome was obvious and known to Defendants, because their public campaign was intended to turn the marketplace against Plaintiff,

as part of Defendants' plan to punish and silence their critics and those associated with their critics.

d. Defendants acted recklessly and in conscious disregard of the risk to Plaintiff, intentionally pursuing their campaign of threats, litigation, and public vilification.

e. Defendants' conduct shocks the conscience because it was motivated by an intent to harm Plaintiff, or at minimum was pursued with deliberate indifference to injuries to Plaintiff that would likely result from Defendants' campaign against Mike Lindell.

110. Defendants are liable to Plaintiff pursuant to 42 U.S.C. § 1983 for the injury inflicted under color of law by them upon Plaintiff, through the deprivation of rights, privileges, and immunities secured by the Constitution, by depriving Plaintiff of property without due process of law in violation of the Fourteenth Amendment.

111. Defendants' deprivation of MyPillow's Constitutional rights, both directly and as a third party, caused injury to MyPillow, including, but not limited to, loss of long-standing business relationships, loss of supplier contracts, loss of promotional access in media, expenditure of attorney fees, emotional distress of employees resulting from threats of verbal attacks, diversion of employee time and attention away from MyPillow, and the chilling of MyPillow's Constitutional right to free speech and expression.

112. Resulting from Defendants' conduct, Plaintiff has suffered damages as described herein.

Count 4
Tortious Interference with Prospective Economic Advantage

113. MyPillow repeats and realleges all allegations set forth above as if they were stated in full and incorporated herein.

114. Defendants intentionally and improperly interfered with Plaintiff's prospective contractual relations by falsely maligning Plaintiff in public, thereby inducing many of Plaintiff's commercial suppliers and buyers to terminate their long-standing relationships with Plaintiff so that Plaintiff lost the benefit of its expected future sales to and from these entities.

115. As detailed in the allegations above, Defendants have intentionally and improperly made false statements about Plaintiff, including, but not limited to, false statements regarding Plaintiff's position on controversial political issues and false statements that Plaintiff authorized and recognized numerous promotional codes that supported various terroristic ideals, groups, or organizations. Defendants also intentionally and improperly filed and widely publicized a frivolous $1.3 billion lawsuit against Plaintiff and publicly threatened to bring additional similar lawsuits against others.

116. As Defendants knew or expected would happen, their intentional and improper actions stirred up public controversy and fear surrounding Plaintiff that caused Plaintiff's commercial suppliers and buyers to dread corresponding controversy and damage to their own reputations if they continued to engage in business with Plaintiff. The sense of negative publicity stirred up by Defendants caused Plaintiff's existing commercial customers, suppliers and buyers, and potential customers, suppliers and buyers, to conclude

that Plaintiff was too reputationally toxic to engage in business transactions with. Further, Defendants' frivolous $1.3 billion lawsuit against Plaintiff caused Plaintiff's current and prospective commercial customers, suppliers and buyers, and potential customers, suppliers and buyers to fear Plaintiff would be unable to continue in its ordinary course of business. Further, Defendants' false publicity campaign caused media companies to terminate Defendants' access to their broadcast and publishing services.

117. The commercial relationships that Plaintiff lost as a result of Defendants' wrongful acts taken without legal justification were in many cases longstanding relationships that Plaintiff had every reasonable expectation would continue to Plaintiff's economic advantage, absent the acts of Defendants.

118. Defendants knew of Plaintiff's business, its manufacturing, and its sales, and knew or should have known Plaintiff had existing commercial customer, supplier and buyer relationships that Plaintiff expected to continue. Yet Defendants intentionally engaged in their tortious and wrongful acts that Defendants knew or should have known would cause the loss of Plaintiff's expected economic advantages through continued commercial supply and sales transactions.

119. Absent Defendants' wrongful acts, Plaintiffs' longstanding successful commercial customer, supplier and buyer relationships would have continued indefinitely.

120. Defendants' wrongful acts have injured Plaintiff, including but not limited to Plaintiff's loss of customer, supplier, and public good will, loss of long-standing business relationships, loss of supplier contracts, and loss of access to promotional access in media. These injuries have caused substantial pecuniary harm to Plaintiff.

121. Resulting from Defendants' conduct, Plaintiff has suffered damages as described herein.

Count 5
Abuse of Process
Against Dominion Defendants

122. MyPillow repeats and realleges all allegations set forth above as if they were stated in full and incorporated herein.

123. On February 22, 2021, Defendants filed a lawsuit against Plaintiff in the United States District Court for the District of Columbia, asserting meritless claims that sought to impose liability on Plaintiff for personal political statements protected by the First Amendment that had been made by Plaintiff's CEO, Mike Lindell. Plaintiff made no statements.

124. Defendants had an ulterior purpose in filing their D.C. Action against Plaintiff. The D.C. Action is merely part of a much larger campaign described above by Defendants who have intentionally sought to intimidate the American public and deter anyone from publicly discussing and commenting on Defendants' services, products, and administration of the 2020 election in any way that was unfavorable to Defendants. Defendants' ulterior purpose was wrongful and improper.

125. By filing and pursuing the D.C. Action, Defendants intentionally sought to make an example of Plaintiff, so that all who learned of the action would fear similar actions being brought against themselves and would not criticize Defendants. Dominion's CEO John Poulos threatened on national television that the D.C. Action against MyPillow was "definitely not the last lawsuit" and that Dominion is "not ruling anyone out."

126. Defendants also mailed copies of the D.C. Action, and other actions they had filed against other parties, to specific individuals whom they sought to intimidate from making statements or providing testimony or sworn statements about the 2020 elections. On information and belief, Defendants filed their action against Plaintiff in part to create litigation papers they could mail out as part of their campaign to block commentary and evidence about the 2020 elections unfavorable to Defendants.

127. Deterrence of public commentary, deterring individuals from providing evidence related to public elections, and deterrence of criticism of Defendants are not proper objectives for the filing of a lawsuit and are not results within the scope of a civil lawsuit. Yet Defendants filed, served, and are pursuing the D.C. Action for the intended malicious purpose of accomplishing these results.

128. Defendants' abuse of the litigation process for these ends is particularly egregious in light of Defendants' governmental role of administering presidential and congressional elections. The sunlight of public discussion, scrutiny, and evidence-gathering is necessary to ensure votes are collected and counted fairly, and to hold those entrusted with administering the process accountable to a high standard of accuracy, security, and reliability.

129. Defendants' abuse of the litigation process has caused extensive injury to Plaintiff, including, but not limited to, loss of long-standing business relationships, loss of supplier contracts, loss of access to promotional access in media, and expenditure of attorney fees defending against the D.C. Action.

130. Defendants are liable to Plaintiff for the injuries it has sustained as a result of Defendants' abuse of process.

131. Resulting from Defendants' conduct, Plaintiff has suffered damages as described herein.

JURY TRIAL DEMANDED

132. Under Rule 38 of the Federal Rules of Civil Procedure, MyPillow demands a trial by jury of all issues so triable in this action.

VI. PRAYER FOR RELIEF

Plaintiff MyPillow requests the following relief:

1. Entry of judgment in favor of MyPillow against Defendants on Counts 1-5 in this Complaint, in an amount to be determined at trial, but at least in an amount that exceeds the jurisdictional limits of this Court;

2. An award of damages to MyPillow for Defendants' unlawful conduct as set forth herein, including a reasonable multiple of enterprise value, exceeding $1.6 billion;

3. An award of damages to MyPillow for the suppression and deprivation of its constitutional rights as set forth herein;

4. An injunction prohibiting any further suppression of speech regarding Dominion's handling of the 2020 election or the integrity of its voting systems;

5. An award of attorneys' fees, costs, expenses, and disbursements;

6. An award of pre-judgment and post-judgment interest on all damages owed to MyPillow; and

7. Such other and further relief as is just and proper.

Dated: April 19, 2021

PARKER DANIELS KIBORT LLC

By */s/ Andrew D. Parker*

Andrew D. Parker (#195042)
Joseph A. Pull (#386968)
Gregory N. Arenson (#398276)
Abraham S. Kaplan (#399507)
888 Colwell Building
123 North Third Street
Minneapolis, MN 55401
Telephone: (612) 355-4100
Facsimile: (612) 355-4101
parker@parkerdk.com
pull@parkerdk.com
arenson@parkerdk.com
kaplan@parkerdk.com

ATTORNEYS FOR PLAINTIFF MY PILLOW, INC. DBA MYPILLOW