United States District Court
District of Minnesota

MICHAEL J. LINDELL,

Plaintiff,

v.

US DOMINION, INC., DOMINION VOTING SYSTEMS, INC., DOMINION VOTING SYSTEMS CORPORATION, SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V., and SGO CORPORATION LIMITED,

Defendants.

Case No._____

COMPLAINT

Jury Trial Demanded

I. OVERVIEW

"We can only spread our knowledge outwards from individual to individual, generation after generation. In the face of the Thought Police, there is no other way."
- George Orwell, *1984*

1. Mike Lindell brings this lawsuit to stop electronic voting machine companies from weaponizing the litigation process to silence political dissent and suppress evidence showing voting machines were manipulated to affect outcomes in the November 2020 general election.

2. Fact: Electronic voting machines and software can be hacked through a cyber attack, thereby allowing data flowing through those devices to be manipulated, stolen, or altered.

3. Fact: It is indisputable that the electronic voting machines and software manufactured and sold by Dominion[1] and Smartmatic[2] are vulnerable to cyberattacks before, during, and after an election, and in a manner that could easily alter election outcomes. Election security expert and University of Michigan science and engineering professor, J. Alex Halderman, and others have given sworn testimony of this fact:[3]

[1] "Dominion Defendants" refers collectively to Defendants US Dominion, Inc., Dominion Voting Systems, Inc., and Dominion Voting Systems Corporation. Unless otherwise noted, "Dominion" refers to Defendant Dominion Voting Systems, Inc.

[2] "Smartmatic Defendants" refers collectively to Defendants Smartmatic USA Corp., Smartmatic International Holding B.V., and SGO Corporation Limited. Unless otherwise noted, "Smartmatic" refers to Defendant Smartmatic USA Corp.

[3] *See* https://www.youtube.com/watch?v=AmivIHUAy8Q

Now-Vice President Kamala Harris, along with other Democratic senators, said the same think during a senate hearing prior to the November 2020 general election:[4]

4. Fact: Direct and circumstantial evidence demonstrates that, during the 2020 General Election, electronic voting machines like those manufactured and sold by Dominion were manipulated and hacked in a manner that caused votes for one candidate to be tallied for the opposing candidate.

5. Fact: Voting machine companies like Dominion are state actors by virtue of their roles running elections in the United States—an essential state function.

6. Fact: The First Amendment guarantees the right of citizens such as Mike Lindell to express political dissent and espouse beliefs without fear of intimidation,

[4] *See* https://www.worldviewweekend.com/tv/video/mike-lindell-presents-absolutely-9-0, beginning at the 22:56 minute mark.

suppression, or punishment from state actors like voting machine companies that provide election equipment and run elections for government agencies.

7. Fact: Following the 2020 General Election, Mike Lindell gathered and publicly shared information from various sources demonstrating that voting machines were, in fact, the target of cyberattacks in the November 2020 general election. Such evidence includes Dr. Douglas Frank's analysis showing conclusively that an algorithm was employed to manipulate votes in the 2020 General Election and evidence of hacking of electronic voting machines by China and other nation-state actors—including twenty such hacks, primarily by actors in China that alone changed the outcomes in the presidential race in the 2020 General Election.

8. Fact: In response to Mike Lindell's public statements about the evidence he had gathered, Dominion Voting Systems and its lawyers at Clare Locke, LLP ("Clare Locke") threatened Mike Lindell with financial ruin if he did not cease his public expression of his political speech regarding the debacle that was the use of electronic voting machines in the 2020 General Election.

9. Fact: When Mike Lindell refused to be intimidated into giving up his First Amendment right to political free speech, Dominion sued him for $1.3 billion in federal court in Washington, D.C.—a jurisdiction where neither Lindell nor Dominion reside, and outside the jurisdiction where Lindell made the vast majority of the statements Dominion complains about.

10. Fact: Dominion has weaponized the legal process and intimidated witnesses to election fraud by suing or threatening to sue over 150 private individuals or

organizations, including dozens of citizen volunteer poll watchers, with baseless defamation lawsuits or "cease and desist" letters from Dominion's lawyers at Clare Locke. Dominion further publicly boasts of doing so—merely because those citizens signed affidavits regarding fraudulent or illegal activities they persoanally observed during the November 2020 general election. Dozens of those citizens *never mentioned* Dominion or issues with any electronic voting machines. Yet, Dominion and Clare Locke still threatened these witnesses—citizen volunteers performing a public service—with ruinous litigation and onerous demands that they preserve even private communications.

11. Fact: Smartmatic has engaged in similar weaponization of the court system to attack other individuals and news outlets, merely for publicly sharing information they have gathered regarding vulnerabilities in, and attacks on, electronic voting machines in the 2020 General Election.

12. Fact: A full forensic audit of the vote in the fourth most populous county in the United States—Maricopa County, Arizona—is currently being conducted. That audit includes an audit of Dominion's voting machines used in that county, as ordered by the Arizona Senate "to restore integrity to the election process." The Maricopa County Board of Supervisors and various Democrat-affiliated groups have spent months attempting to thwart or obstruct the audit—efforts that have been repeatedly rebuffed in Court. This includes refusing to turn over routers to which the Dominion machines were connected and which will show details regarding the Dominion machines' connectivity to the internet. The Maricopa County officials have also admitted they do not possess the administrative passwords to the Dominion voting machines—meaning Dominion employees had control

over the election. Dominion joined the Democrat-led chorus to smear the audit and has refused to cooperate with the auditors, including refusing to turn over the administrator passwords to the voting machines.

13. Fact: Forensic audits and investigations of the November 2020 election and the role of voting machines and electronic voting systems are currently underway either by court order or by direction of state legislatures or attorneys general in Arizona, Georgia, Michigan, Wisconsin, and New Hampshire.

14. Conclusion: Dominion, Smartmatic, and others are desperate to cover up gross security flaws in their electronic voting systems—and information showing cyber attacks and hacking in the November 2020 election—by uniting in a common purpose to use the litigation process to attempt to suppress the revelation and public discussion of these truths.

15. This new, fledgling era of "lawfare"[5] must be stopped before it is allowed to gain a toehold of acceptance in the U.S. judiciary and the courts become yet another weapon for wealthy corporations and the powerful politicians they support to silence speech and ideas they deem unacceptable to their narrative.

II. PARTIES

16. Plaintiff Michael J. Lindell ("Plaintiff" or "Lindell") is an individual citizen of the State of Minnesota.

[5] Lawsuit Warfare = Lawsuit + Warefare = Lawfare. *See* https://en.wikipedia.org/wiki/Lawfare

17. Defendant US Dominion, Inc. is a corporation organized and existing under the laws of the State of Delaware with its principal place of business in Denver, Colorado. It may be served with process by delivering the summons and complaint to its Chief Executive Officer, John Poulos, at its principal place of business, 1201 18th Street, Suite 210, Denver, Colorado 80202.

18. Defendant Dominion Voting Systems, Inc. is a corporation organized and existing under the laws of the State of Delaware with its principal place of business in Denver, Colorado. It may be served with process through its registered agent for service of process in Minnesota, Cogency Global, Inc., 6160 Summit Drive N., Suite 205, Brooklyn Center, Minnesota 55430.

19. Defendant Dominion Voting Systems Corporation is a corporation organized and existing under the laws of the Province of Ontario, Canada with its principal place of business in Toronto, Ontario, Canada. It may be served with process in accordance with the terms of the Hague Convention.

20. Defendant Smartmatic USA Corp. is a corporation organized and existing under the laws of the State of Delaware with its principal place of business in Boca Raton, Florida. It may be served with process by delivering the summons and complaint to its Director, James Long, at its principal place of business, 1001 Broken Sount Parkway, Suite D, Boca Raton, Florida 33487.

21. Defendant Smartmatic International Holding B.V. is a corporation organized and existing under the laws of the Netherlands, with its principal place of business in

Amsterdam, Netherlands. It may be served with process in accordance with the terms of the Hauge Convention.

22. Defendant SGO Corporation Limited is a corporation organized and existing under the laws of the United Kingdom with its principal place of business located in London, United Kingdom. It may be served with process in accordance with the terms of the Hague Concention.

III. JURISDICTION AND VENUE

23. This Court has jurisdiction over the subject matter of this dispute pursuant to 28 U.S.C. § 1331, in that one or more of Plaintiff's causes of action arises under the Constitution or laws of the United States. Specifically, Plaintiff alleges causes of action under 42 U.S.C. § 1983, 42 U.S.C. § 1985(3), and 18 U.S.C § 1964.

24. This Court also has jurisdiction over the subject matter of this dispute pursuant to 28 U.S.C. § 1332, in that the matter in controversy exceeds $75,000, exclusive of interest and costs, and is between citizens of different states or citizens of a State and citizens or subjects of a foreign state. Specifically, Lindell is a citizen of Minnesota, while Defendants are citizens of Delaware, Colorado, Florida, Canada, the Netherlands, and the United Kingdom.

25. This Court has *in personam* jurisdiction over Defendants in that Defendants have minimum contacts with the State of Minnesota, having purposefully availed themselves of the privilege of doing business here. Moreover, this Court's assertion of personal jurisdiction over Defendants comports with traditional notions of fair play and substantial justice.

26. Venue is proper in this District under 28 U.S.C. § 1391 in that Defendants are subject to personal jurisdiction in this District, as set out above.

IV. FACTUAL ALLEGATIONS

"Power is in tearing human minds to pieces and putting them together again in new shapes of your own choosing."

- George Orwell, *1984*

27. Lindell will prove that the Dominion Defendants, acting in concert and as part of an unlawful enterprise alongside the Smartmatic Defendants, have weaponized the court system and the litigation process in an attempt to silence Lindell's and others' political speech about election fraud and the role of electronic voting machines in it. In the specific context of political speech about something as vital to a republican form of government as election integrity, no litigant should be permitted to use the courts and the litigation process as a bludgeon to suppress and stifle dissent. But that is what the Dominion Defendants and Smartmatic Defendants have done. Many of their victims lack the resources to fight back and expose the defendants' scheme for what it is—an authoritarian abuse of state power fueled by the virtually unlimited resources from their ideological comrades. But Mike Lindell has the resources and the will to fight back, albeit at great personal and financial cost; Mike Lindell believes the future of the American republic depends on fighting back against censorship of information concerning the fundamental aspect of our republic—fair and secure elections. So Mike Lindell brings this suit to bring a stop to the defendants' abuses of the legal system and protect Americans' right to speak freely on matters of the utmost public concern.

A. The Rise of the Machines

"You talk as if a god had made the Machine … I believe that you pray to it when you are unhappy. Men made it, do not forget that."

- E.M. Forster, *The Machine Stops*

28. Prior to 2002, states conducted their elections overwhelmingly using relatively secure and auditable paper-based systems. However, following passage of the Help America Vote Act in 2002,[6] billions of federal dollars were spent to move from such paper-based systems to electronic, computer-based systems.

29. As a result, by 2020, most elections in the United States were conducted using one of only a small handful of available private election management systems. These systems are provided by a small number of private companies having little to no transparency to the public, producing results that are far more difficult to audit than paper-based systems, and lacking any meaningful federal standards or security requirements beyond what individual states may choose to certify.[7]

30. This small cadre of private companies supply the hardware and software for the election management systems and electronic voting machines, in some cases manage the voter registration rolls, maintain the voter records, partially manage the elections, program the vote counting, and report the election results to the relevant government authorities.

[6] 52 U.S.C. § 20901 *et seq*.

[7] Dominion touts its certification by the United States Election Assistance Commission ("EAC"). But as of November 2020, the EAC did not test or certify electronic voting systems for security against cyberattacks.

31. A total of five (5) companies conduct and administer elections for more than ninety percent (90%) of counties in the United States: (1) Election Systems & Software, (2) Dominion Voting Systems, (3) Smartmatic USA Corp., (4) Hart InterCivic, and (5) Tenex. All these providers' electronic voting machines and election management systems are vulnerable to hacking, as has been published and presented to various congressional committees. All can be, and at various steps in the voting, counting, tabulation, and/or reporting process are designed to be, connected to the internet directly or indirectly.

32. After votes are tabulated at the county level using one of the handful of available election management systems, they are then uploaded over the internet to one of a small handful of election night reporting systems. Those systems are owned and controlled by Scytl, GCR, VR Systems, and Arikkan. For its part, the Clarity system, used in 28 states, is wholly owned by Scytl, a multi-national company headquartered in Barcelona, Spain that reportedly stores its election vote data on servers in Frankfurt, Germany.

33. In short, over the last two decades, the United States has transitioned from a safe, secure, auditable paper-based system (paper voter rolls, hand-marked paper ballots, etc.) to an inherently vulnerable, internet-exposed electronic voting machine-based system. And not surprisingly, that transition to increased reliance on electronic systems and computer technology has brought with it the very real spectre of hacking, election tampering, and electronic voting fraud.

34. As previously noted, Dominion and Smartmatic manufacture, distribute, and maintain 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.

35. 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.

36. Increasingly, jurisdictions have chosen to outsource election operations and programming to private contractors. By the time of the 2020 election, at least 3,143 counties across the United States had outsourced responsibility for programming and administering elections to private contractors. For the 2020 election, Dominion provided its voting machines and services in more than half of the United States from its U.S. base of operations in Colorado. 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.

37. 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."[8] 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. By contracting with governmental jurisdictions to provide comprehensive voting solutions for public elections, Dominion is a governmental actor. As a result of Dominion's contracts with government entities, it is delegated responsibility to administer public elections, including the election of individuals to serve in constitutionally prescribed offices—a core governmental function. In at least one jurisdiction in the November 2020 election, Maricopa County, Arizona, county officials did not even possess the administrator passwords to the Dominion voting machines—meaning only Dominion could program and operate the machines on behalf of the county.

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

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

B. Strange Bedfellows

"Misery acquaints a man with strange bedfellows."
- William Shakespeare, *The Tempest*

39. Dominion and Smartmatic both manufacture, distribute, and maintain voting hardware and software. They both also execute software updates, fixes, and patches for their voting machines and election management systems. On the surface, Dominion and Smartmatic appear as competitors in the market for electronic voting systems. But in reality, they share many things in common—including an intertwined corporate history and a shared "DNA" of election management system software and hardware. They also share a common purpose of using litigation and "lawfare" to silence any who would publicly criticize the security flaws in their voting machines and systems or attempt to inform the public about the role of those flaws in undermining the integrity of the 2020 presidential election.

40. According to its website,[9] Dominion was founded in 2003, and provides electronic voting machines and systems in 28 different states and Puerto Rico, including "9 of the top 20 counties" and "4 of the top 10 counties" in the United States. Its machines and systems range from the "election event designer"—software that creates the ballots voters will mark while voting, as well as programing the tabulators of those votes—to the devices on which voters mark their votes ("ballot marking devices," or "BMDs"), to the machines that tabulate the votes at the precinct level, to the machines that receive and tabulate the various precinct results ("centralized tabulation"), to the systems and options

[9] https://www.dominionvoting.com

for transmitting those results from the BMD to the precinct tabulator to the central tabulator to, ultimately, the official government authority responsible for certifying the election results. In a very real sense, then, Dominion controls the administration and conduct of the elections in those jurisdictions where its systems are deployed, and any vulnerabilities or weaknesses in Dominion's systems undermine—or at the very least, call into legitimate question—the integrity and reliability of all election results coming from those jurisdictions.

41. According to its website,[10] Smartmatic was founded in 2000 in Palm Beach County, Florida, and developed its first electronic voting machine in 2003. However, it finds its true beginnings in Venezuela back in 1997, when three Venezuelan engineers—Antonio Mugica, Alfredo Jose Anzola, and Roger Piñate founded Tecnologia Smartmatic de Venezuela, C.A. It was not until April 2000 that the founders created Smartmatic Voting Systems in Delaware, with headquarters in Boca Raton, Florida. But Smartmatic's ties to Venezuela remained strong. In early 2004, a Venezuelan government financing agency invested more than US $200,000 in a technology company, Bitza, owned by the same owners as Smartmatic. Also in 2004, Smartmatic was contracted by the Venezuelan National Electoral Council to provide e-voting technology for the 2004 Venezuelan national elections. That same year, Smartmatic moved its headquarters to Amsterdam, the Netherlands.

[10] https://www.smartmatic.com/us/about/our-history/

42. In 2005, Smartmatic opened its research and development center in Taipei, Taiwan, and also began to offer its electronic voting services in the United States. Between 2007 and 2008, Smartmatic expanded its offerings to numerous foreign jurisdictions, including Curaçao, the Phillipines, Argentina, and Brazil, while continuing its close relationship as a contractor for the Hugo Chavez-controlled government of Venezuela. By 2011, Smartmatic had expanded its operations to Mexico, Haiti, Panama, and India. In 2012, Smartmatic moved its headquarters to London. In 2014, Smartmatic created the Centre for Excellence in Estonia with the goal of advancing internet voting. By 2015 and 2016, Smartmatic was offering its electronic voting services in such far-away jurisdictions as Sierra Leone, Kyrgyzstan, Uganda, and Oman. In 2018, Smartmatic became a member of the United States Department of Homeland Security's fledgling Sector Coordinating Council for the Election Infrastructure Sector[11]—a prime example of "the fox guarding the henhouse."

43. The histories of Dominion and Smartmatic are inextricably intertwined, which helps to explain their coordinated actions at issue in this lawsuit. Some background is important to understand this point.

44. From roughly 2002 to 2009, two voting machine vendors dominated electronic voting in United States elections: Diebold Election Systems (re-branded to Premier Election Solutions, Inc. in 2007) and Election Systems & Software ("ES&S").

[11] *See* https://www.smartmatic.com/us/media/article/smartmatic-founding-member-of-the-dhs-council-to-protect-election-integrity-and-security/

ES&S was acquired by American Information Systems ("AIS"), a company formed in Nebraska by the Urosevich brothers, descendants of Serbian immigrants.[12] Following that acquisition, AIS changed its name and began doing business as ES&S. From 2002 to 2009, ES&S served approximately 45% of precincts in the United States, while Diebold (operating under the Premier name) served approximately 23% of U.S. precincts. The remaining precincts were served by Sequoia Voting Systems (18%), Hart InterCivic (9%), and Dominion (founded in 2003) (5%).

45. In 2005, Smartmatic (flush with cash from its 2004 efforts on behalf of the Hugo Chavez government in Venezuela) acquired Sequoia for $16 million and, with it, its 18% U.S. electronic voting market share. Smartmatic worked quickly to replace Sequoia's inferior technology with Smartmatic's own systems and personnel, which was followed by two years of rapid growth and solid revenue. Then, concerns arose about the ties between Smartmatic/Sequoia and the government of Venezuela. Specifically, in or around May 2006, Congresswoman Carolyn Maloney (D. NY) asked the U.S. Treasury Department to investigate Smartmatic's acquisition of Sequoia. Around the same time, concerns arose in connection with Smartmatic's efforts to implement its systems for the City of Chicago, when observers noticed that Smartmatic was flying in developers from Venezuela to

[12] Dominion's ties to Serbia run far deeper than the ancestry of AIS's founders. In May 2016, Dominion's then Vice President, Goran Obradovic, gave an interview in which he stated that Dominion's office in Belgrade was opened in 2005 and had grown by 2016 into a team of 50 engineers. "The products such as Democracy Suite Election Management System, ImageCast Evolution and ImageCase X **are completely developed in Belgrade."** https://ekonomijaibiznis.mk/ControlPanel/Upload/Free_Editions/wZ0X5bz60KCgpcvFcEBvA/maj%202016%20ENG/mobile/index.html#p=33 (emphasis added).

resolve issues and assist with the implementation. By the time those concerns emerged publicly in the U.S. media, Sequoia/Smartmatic had voting equipment located in 17 U.S. states and the District of Columbia.

46. Concerned for the integrity of their elections and voting system, the Committee on Foreign Investment in the United States ("CFIUS") ordered an audit to determine if any Foreign Investment Act rules had been broken. However, rather than undergoing that audit, Smartmatic developed a plan to divest (sell) Sequoia to its U.S.-based management, and establish Smartmatic as a U.S.-based provider of global election systems. To that end, in late 2007 or early 2008, Smartmatic and Sequoia management formed a new company, SVS Holdings, which became the new owner of Sequoia. However, Smartmatic continued to hold a promissory note from SVS secured by $2 million worth of shares, along with a percentage "earn-out" from future SVS revenues. Moreover, Smartmatic's technology continued to be used in SVS/Sequoia machines.

47. In 2009, ES&S acquired Premier, creating a market behemoth with nearly 70% of the market share for electronic voting systems in the United States. Not long after the acquisition anti-trust concerns led to ES&S being forced to divest itself of Premier. In May 2010, ES&S sold Premier to Dominion, then a Canadian company with only 5% of the United States market for electronic voting systems. According to Dominion's press release at the time, the acquisition included "the primary assets of Premier, including all intellectual property, software, firmware and hardware for Premier's current and legacy optical scan, central scan, and touch screen voting systems,and all versions of the GEMS election management system."

48. In June 2010, under continued pressure from authorities due to the ongoing financial and technological control by Smartmatic, SVS was forced to sell Sequoia and its Smartmatic-heavy technology. The buyer? None other than the upstart Canadian company, Dominion. Dominion thereby acquired Sequoia, including the rights to the Smartmatic technology still used in SVS/Sequoia machines following the Sequoia divestiture from Smartmatic in or around 2005. After the acquisition of Sequoia, Dominion held roughly 50% of the private electoral market for electronic voting in the U.S., with only two remaining competitors—ES&S, with 40%, and Hart InterCivic, with 10%. At the time, Dominion spokesman Chris Rigall claimed that "Smartmatic's intellectual property was not included in the Sequoia transaction because Sequoia did not own it." But according to a 2017 report published by the *Huffington Post*, "The 'intellectual property' of the voting systems (of Sequoia, acquired by Dominion) remains the property of the company linked to the Venezuelan president (Smartmatic and Hugo Chavez), despite the rather misleading statement" issued by Dominion in 2010. In fact, the *Huffington Post* investigation revealed that the intellectual property "of most/almost all of Sequoia's voting systems was actually secretly owned by the firm Smartmatic." It was later discovered that Smartmatic still held interests in Sequoia, even controlling the company's intellectual property through rights it had reserved to negotiate by means of non-compete agreements abroad.

49. The historically intertwined relationship between Dominion and Smartmatic extends beyond the mere acquisition of legacy hardware and software technologies. For example, in 2009, Dominion and Smartmatic entered into a license agreement whereby

Smartmatic leased from Dominion certain precinct count optical scan technology, including "the right to market, make, use and sell PCOS voting systems using the Dominion technology," as well as "the applicable hardware, software and firmware loaded on the hardware and election management system ('EMS') software designed to be used with such version of the PCOS system."

50. Even more telling is the cross-pollenization of former Smartmatic employees and inventors who found their way to Dominion in the Sequoia acquisition. With Dominion's acquisition of Sequoia in June 2010, came Eric Coomer, Vice President for Engineering at Smartmatic, and Frederico Arnao, Venezuelan-born "Usability Architect" for Smartmatic and Senior Software Developer for Smartmatic-affiliated Bizta Voting Systems. Importantly, Arnao and Coomer are named as inventors on a pair of patent applications filed on April 22, 2011, dealing with electronic voting systems, claiming priority to patents filed in 2009, while they were still employed by Smartmatic. (For his part, Coomer is listed as an inventor on an additional four such patents, one of which traces back to a patent filing in 2008.) By way of further example, public internet searches identify at least four additional employees who are shown as employees of Dominion Voting Systems at Smartmatic's Boca Raton, Florida business address, with @smartmatic email addresses:

Name	Title	Company	E-mail	Address	Web Domain
Babic, Paul	Vice President Marketing	Dominion Voting Systems Corp, Boca Raton, Florida	Paul.babic@smartmatic.com	1001 Broken Sound Pkwy NW, Boca Raton, FL 33487	Dominionvoting.com
Cook, Jason	U.S. Sales	Dominion Voting Systems Corp, Boca Raton, Florida	Jason.cook@smartmatic.com	1001 Broken Sound Pkwy NW, Boca Raton, FL 33487	Dominionvoting.com
Scott, Jeffrey	Senior Technical Sales Engineer	Dominion Voting Systems Corp, Boca Raton, Florida	Jeff.scott@smartmatic.com	1001 Broken Sound Pkwy NW, Boca Raton, FL 33487	Dominionvoting.com
Vasquez, Jorge M.	Vice President Operations	Dominion Voting Systems Corp, Boca Raton, Florida	jvasquez@smartmatic.com	1001 Broken Sound Pkwy NW, Boca Raton, FL 33487	Dominionvoting.com

51. Legislators have long raised questions about the murky picture of who exactly owns and controls electronic voting machine companies like Dominion. In December 2019, United States Senators Elizabeth Warren (D-Mass.), Amy Klobuchar (D-Minn.), Ron Wyden (D-Or.), and Congressman Mark Pocan (D-Wis.) wrote to Stephen D. Owens and Hootan Yaghoobzadeh, Managing Directors of Staple Street Capital, LLC, a private equity firm, which acquired Dominion in 2018. After recognizing that Dominion was "one of three election technology vendors responsible for developing, manufacturing and maintaining the vast majority of voting machines and software in the United States, the four Democratic congressional leaders raised a number of serious concerns regarding "the spread and effect of private equity investment in many sectors of the economy, including the election technology industry—an integral part of our nation's democratic process." Those concerns included:

a. "[T]hat secretive and 'trouble-plagued companies,' owned by private equity firms and 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.'"

b. "[T]hree large vendors—Election Systems & Software, Dominion, and Hart InteCivic—collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States."

c. "Election security experts have noted for years that our nation's election systems and infrastructure are under serious threat."

d. "[V]oting 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."

e. "[R]esearchers recently uncovered previously undisclosed vulnerabilities in 'nearly three dozen backend election systems in 10 states.'"

f. "These problems threaten the integrity of our elections and demonstrate the importance of election systems that are strong, durable, and not vulnerable to attack."

The congressional leaders' letter followed these concerns with a request for seven specific categories of information "[i]n order to help us understand your firm's role in this sector."

52. The congressional leaders' concerns were not unfounded. In 2018, Dominion was acquired by a private equity firm, Staple Street Capital, whose largest shareholder, David Mark Rubenstein, is a co-founder of The Carlyle Group. The Carlyle Group is a global investment firm with longstanding and enormous investments in China. In 2020, mere months before the election, Staple Street Capital (owner of Dominion) received a $400 million investment from UBS Securities, LLC. UBS Securities LLC owns 24.99% of UBS Securities Co. LTD, a Chinese investment bank. The remaining 75% of UBS Securities Co. LTD is owned by the Chinese government or various arms of it. At

the time of the November 2020 election, the two UBS Securities affiliates shared three common directors: (1) Ye Xiang (Board Chairman of UBS Beijing until his resignation in December 2020, also Secretary of Peoples Bank of China and ex-director of Bank of China International); (2) Mu Lina (Director of Fund Management and Head of Fund Operations for UBS Beijing); and (3) Luo Qiang.

53. Nor do the connections between Dominion, Smartmatic, and China end with the $400 million investment in Dominion's parent. Five years earlier, beginning in 2015, Smartmatic began using the Chinese company Shenzhen Zhongjian Nanfang Testing Co., Ltd. to conduct in-depth testing, studies, and certifications of its voting machine hardware and software. This relationship continued until at least 2020, just prior to the election. In that role, the Chinese company had complete access to all facets of Smartmatic's devices and software—which shared the same "DNA" as the Dominion systems going back to the Diebold-Premier-Sequoia acquisitions. Worse still, in or around September 2019, Dominion pledged as many as eighteen of its patents as collateral with Hong Kong Shanghai Banking Corporation (HSBC), a large Chinese bank.

54. In other words, by the time of the 2020 election, Chinese government-related entities, Chinese technology companies, and powerful Chinese financial interests had direct or indirect ownership of and near-total access to Dominion's and Smartmatic's voting machine technology. Small wonder that by then congressional leaders had serious concerns regarding "the spread and effect of private equity investment in many sectors of the economy, including the election technology industry."

C. Ghosts in the Machines

"But you can't make people listen. They have to come round in their own time, wondering what happened and why the world blew up around them. It can't last."
- Ray Bradbury, *Fahrenheit 451*

55. As a result of systemic and well-documented 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.

56. Lindell was not the first to sound the alarm that electronic voting machines posed grave threats to U.S. election integrity. Indeed, voices from the political left had been protesting the use and vulnerability of electronic voting machines for years prior to the 2020 Presidential election.

57. 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 were wide-open to hacking. Evidence that Dominion's voting systems actually were hacked in the 2020 election continues to accumulate.

58. 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."[13] Recently, the New Hampshire

[13] Press Release, Ariz. Senate Republicans, Senate chooses qualified auditing firm to conduct forensic audit of Maricopa County election results (Jan. 29, 2021)

Senate voted 24-0 to conduct a complete examination of Dominion-owned voting machines after suspicious shorting of votes was discovered.[14] Litigation involving Dominion's voting machines in Antrim County, Michigan, initiated after approximately 6,000 votes were discovered to have been wrongly switched between Presidential candidates—ostensibly due to a so-called "glitch"[15]—proved Dominion's machines could be manipulated and hacked to generate this "glitch."

59. During a December 30, 2020 live-streamed hearing held by the Georgia Senate Judiciary Subcommittee on Elections, a testifying expert hacked into a Dominion polling pad during a live broadcast to the world.[16] And, at the same hearing, legislators were shown replays of real-time news reports showing that tens of thousands of votes were switched from President Trump to former Vice President Biden in several counties in Georgia. For example, in Bibb county, Trump was reported to have 29,391 votes at 9:11 pm EST while simultaneously former Vice President Biden was reported to have 17,218

---

https://www.azsenaterepublicans.com/post/senate-chooses-qualified-auditing-firm-to-conduct-forensic-audit-of-maricopa-county-election-results.

[14] 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.

[15] 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/.

[16] 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/.

votes. A minute later at the next update, these vote numbers switched, with Trump now having 17,218 votes and Biden having 29,391—a 12,173-vote switch in Biden's favor. YouTube—owned by Google, Inc.—removed this news video after this switch was revealed.[17] No rational explanation has ever been offered showing a legitimate reason for this switch in the vote tally.

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

61. As noted, Dominion purchased Premier (formerly Diebold) from ES&S in 2010, 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). [18]

62. Premier had been owned by Diebold, but Diebold changed its name to Preimier in 2007 after a series of studies publicized its unreliable security and accuracy, and technical problems sullied its reputation. The name change was motivated by the desire to create a fresh public image.[19] Diebold sold Premier to ES&S for $5 million in September

[17] https://epochtimes.today/georgia-data-shows-24658-of-trumps-votes-removed-another-12713-switched-to-biden-data-scientists/.

[18] "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-.

[19] 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/.

2009, reporting a $45 million loss,[20] and nine months later, in May 2010, ES&S sold Premier to Dominion.

63. The Diebold technology Dominion obtained when it acquired Premier has 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.[21]

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 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."[22]

[20] 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/.
[21] 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/.
[22] *Id*.

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."[23] 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 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

[23] 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).

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."[24]

e. The Princeton team prepared a video demonstration showing how malware could shift votes cast for one candidate to another.[25] 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.[26]

64. Despite these security weaknesses, Dominion incorporated GEMS into its voting machines after acquiring the technology in 2010. By 2011, Dominion Voting Systems was selling voting systems that had updated GEMS software at the core of their DNA.[27]

---

[24] 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).

[25] *See Security Demonstration of DieBold AccuVote-TS Electronic Voting Machine*, YOUTUBE (Nov. 30, 2016) https://www.youtube.com/watch?v=B8TXuRA4IQM&t=20s.

[26] *See id.*

[27] 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),

65. Vote integrity issues with Dominion's voting systems predated its acquisition and incorporation of GEMS, both in the U.S. and abroad. In 2009, during a New York congressional election, Dominion's software allowed voters to vote for more than one candidate, and its faulty machines froze during operation due to insufficient memory.[28] In the 2010 general election in the Philippines, allegations of technical problems and offers of vote manipulation were rampant.[29] In that election, where Dominion's products were in more than 2,200 local municipalities, a Dominion "glitch" caused voting machines to incorrectly read ballots, while poll machines supplied by Smartmatic had wrongly configured flash cards affecting the automated count.[30] A Product Manager of Dominion indicated that more than 76,000 compact flash cards had to be configured just days before the election.

66. Dominion continued selling and leasing the troubled AccuVote voting machine as recently as 2017.[31]

---

https://files.floridados.gov/media/697908/dominion-gems-release-1216-version-1-test-report.pdf (Ex. 3).

[28] *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.

[29] *See, e.g.,* Reuters, "Aquino unfazed by Philippine poll fraud allegations," May 27, 2010, https://www.reuters.com/article/idINIndia-48840420100527

[30] 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.

[31] *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.

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

68. 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."[32] 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*, 493 F.Supp.2d 1264, 1267 (N.D. Ga. 2020).

69. On October 11, 2020, just three weeks before the 2020 general election, Judge Amy Totenberg[33] issued an order regarding the Dominion voting system's security risks and the potential for fraud or irregularities.[34] 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

[32] Amended Complaint, Doc. 15, N.D. Ga. No. 2017CV292233 (Ex. 4).
[33] Given the hyper-partisan nature of the allegations and assertions set forth in Dominion's Complaints against Lindell and others, it is worth noting that Judge Totenberg was nominated to the federal bench by President Obama in January of 2011.
[34] *Curling v. Raffensperger*, No. 493 F.Supp.d 1264, 1267 (N.D. Ga. 2020) (Ex. 5).

happen?' – but 'when it will happen,' especially if further protective measures are not taken."[35]

70. Judge Totenberg's findings reflected many of the same issues which had existed more than ten years earlier with the predicate Diebold GEMS 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."[36]

71. Although Judge Totenberg declined the *Curling* plaintiffs' request for injunctive relief requiring paper ballots—because she felt bound by Eleventh Circuit

[35] *Id*. at 1342.
[36] *Id*. at 1278, 1280, 1281, 1283, 1287, 1306.

precedent and because there was insufficient time to implement the requested relief prior to the election—she nevertheless 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. [37]

72. In addition to her December 2019 letter to Dominion's parent company, Staple Street Capital, Senator Warren noted how Dominion kept their operations under a cloak of secrecy: "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. They also share little or no information regarding annual profits or executive compensation for their owners."[38]

---

[37] *Id*. at 1341-42.

[38] *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.

73. 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."[39]

74. 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."[40]

75. After failing certification in Texas in January 2019, on October 2 and 3, 2019, Dominion again presented its Democracy Suite 5.5-A voting system in Texas for examination and certification.[41] It failed the second time as well.

---

[39] 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.

[40] 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.

[41] 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. 6).

76. "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.[42]

77. 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."[43, 44] "[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."[45] Other security vulnerabilities found by Texas include use of a "rack mounted server" which "would typically be in a room other than a room used for the central count" and would present a security risk "since it is out of sight."[46]

---

[42] *Id.*
[43] Letter from Brandon Hurley to Keith Ingram (Feb. 19, 2019) (Ex. 7).
[44] 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.
[45] 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.
[46] *Id.*

78. 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."[47]

79. 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.[48] 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**."[49] This is false.

80. For example, in his May 2016 interview, Dominion Vice President Obradovic stated, "All devices of the ImageCast series have additional options such as modems for wireless and wired transfer of results from the very polling place…."[50]

81. Dominion has even tried to hide its systems' internet connectivity from the election officials who are ostensibly in charge of running the elections where Dominion's systems are used. *Vice* reported in 2019, "[A] group of election security experts have found

---

[47] 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/.

[48] 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.

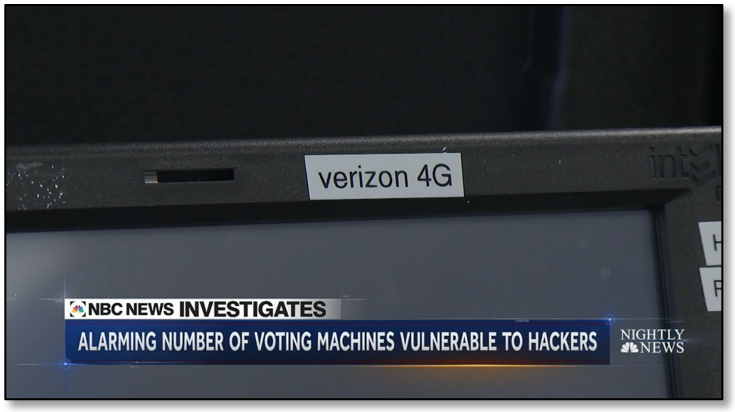
[49] *See* https://danfromsquirrelhill.wordpress.com/2020/12/31/oomf/ (emphasis added). Again, Google's YouTube deleted this video shortly after it began to gain circulation.

[50] https://ekonomijaibiznis.mk/ControlPanel/Upload/Free_Editions/wZ0X5bz60KCgpcvFcEBvA/maj%202016%20ENG/mobile/index.html#p=33

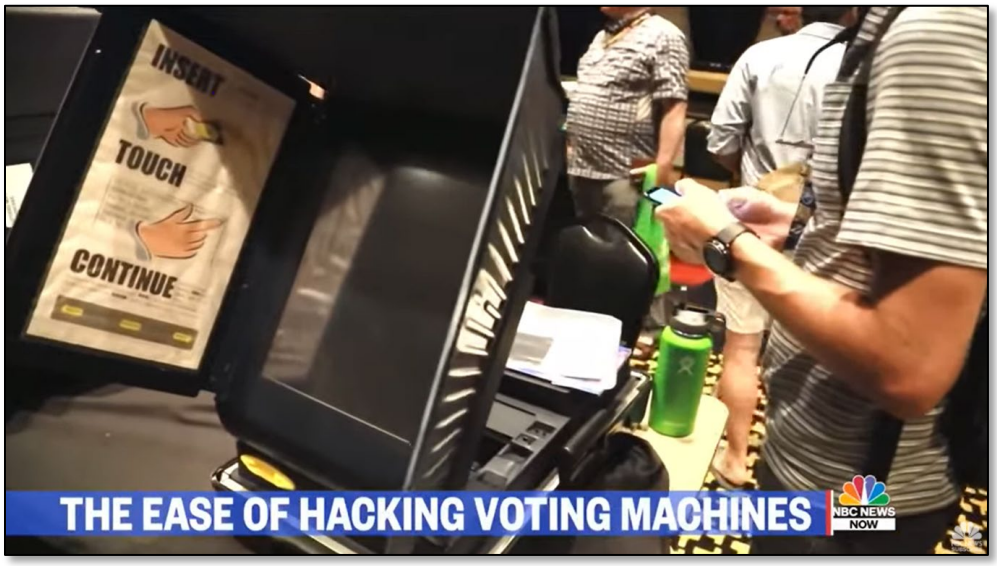
what they believe to be nearly three dozen backend election systems in 10 states connected to the internet over the last year, including some in critical swing states. These include systems in nine Wisconsin counties, in four Michigan counties, and in seven Florida counties. . . . [A]t least some jurisdictions 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**."[51] In 2020, a team of election security experts found more than 35 voting systems were online.[52]

82. 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."[53]

[51] *Id*. (emphasis added).
[52] 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.
[53] *Id.*

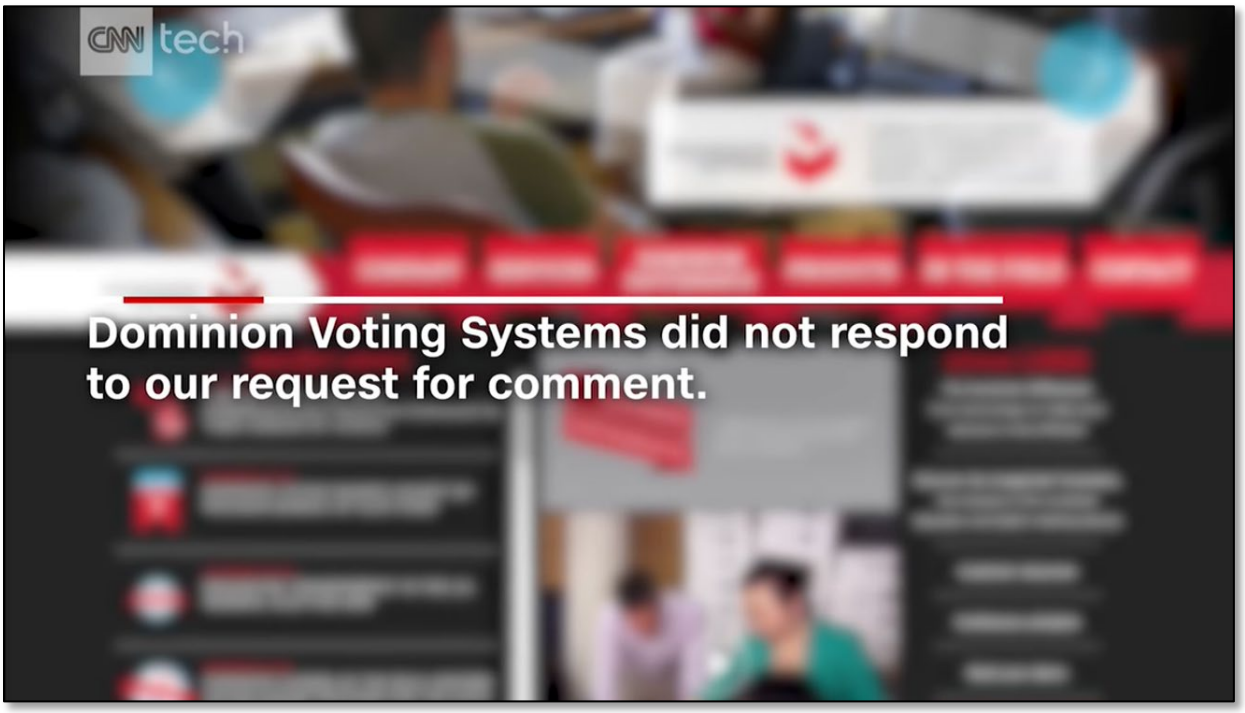


83. In a 2019 story about the DEF CON hacking conference, NBC News reported that Dominion avoided participation in the conference; that hackers can target voting systems with ease; and that Dominion's voting machines are connected to the internet.[54]



[54] NBC News, *How Hackers Can Target Voting Machines | NBC News Now*, YouTube (Aug. 12, 2019), https://www.youtube.com/watch?v=QtWP0KDx2hA.

84. In 2017, Dominion refused to respond to CNNTech's request for comment about its hackable voting machines.[55] 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. . . ."[56]



85. The Congressional Task Force on Election Security's Final Report in January 2018 identified the vulnerability of U.S. elections to foreign interference:[57] "According to DHS, Russian agents targeted election systems in at least 21 states, stealing personal voter

[55] CNN Business, *We watched hackers break into voting machines*, YouTube (Aug. 11, 2017), https://www.youtube.com/watch?v=HA2DWMHgLnc.
[56] *Id.*
[57] CONGRESSIONAL TASK FORCE ON ELECTION SECURITY, FINAL REPORT (2018) (Ex. 8).

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.'"[58]

86. 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."[59]

87. In 2016, "Russian agents probed voting systems in all 50 states, and successfully breached the voter registration systems of Arizona and Illinois."[60] 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

---

[58] *Id*. at 6-7.

[59] *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).

[60] 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.

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."[61]

88. 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 for a different candidate."[62] 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.]"[63]

89. HBO's documentary *Kill Chain: The Cyber War on America's Elections*,[64] details the vulnerability of election voting machines, including Dominion's. Harri Hursti,

---

[61] 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.

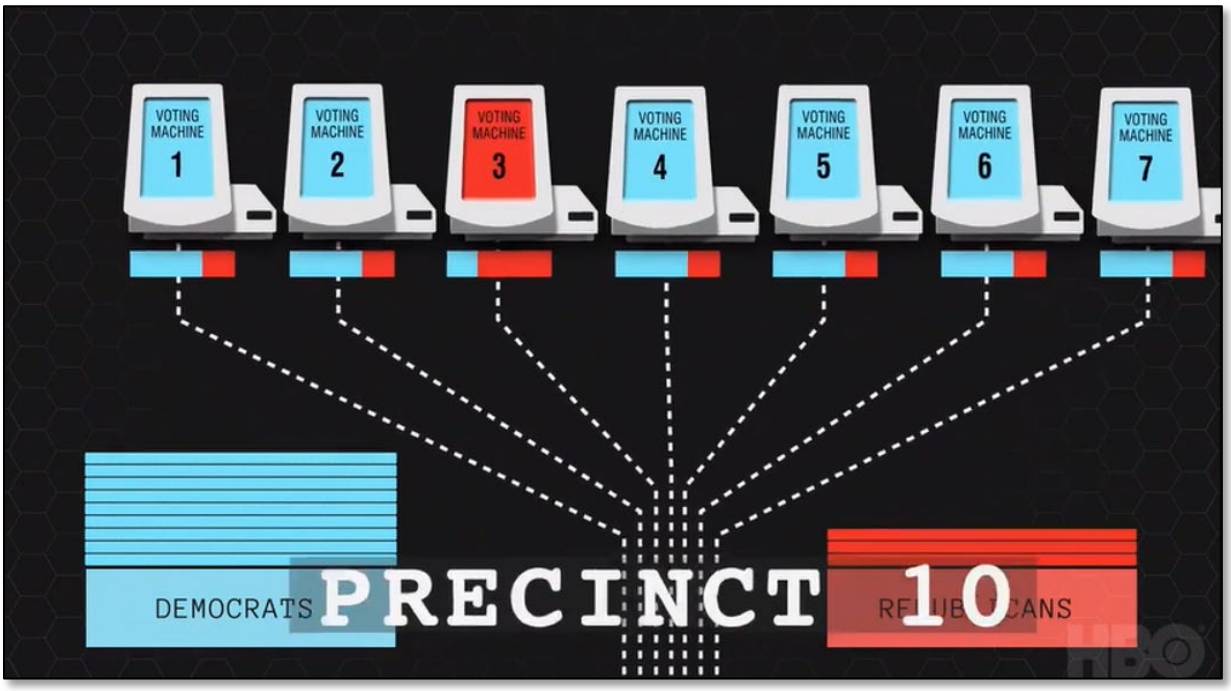
[62] Lawrence Norden and Christopher Famighetti, *AMERICA'S VOTING MACHINES AT RISK*, Brennan Ctr. for Just., 13 (Sep. 15, 2014), available at https://www.brennancenter.org/sites/default/files/2019-08/Report_Americas_Voting_Machines_At_Risk.pdf (Ex. 9).

[63] *Id.*

[64] 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.

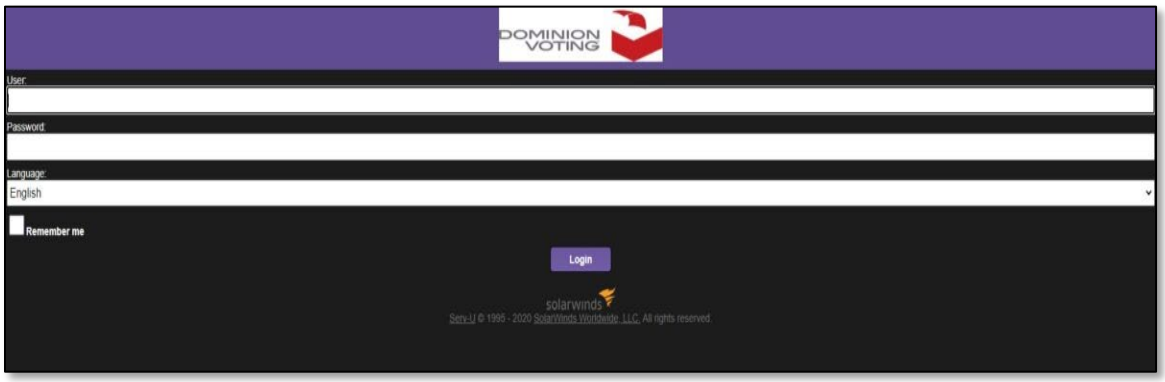
a world-renowned data security expert, showed that he hacked digital voting machines to *change votes* in 2005. According to Hursti, the same Dominion machine that he hacked in 2005 was slated for use in 20 states for the 2020 election.

90. 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, Department of Statistics, UC Berkeley, stated the likelihood of this happening is "an astronomically small chance." It was less than one in a million.[65]



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

91. In December 2020, the Department of Homeland Security's Cybersecurity & Infrastructure Agency ("CISA") revealed that hackers infiltrated SolarWinds software.[66] 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.



92. 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.

[66] 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.

D. Gaslighting: The REAL Big Lie

"And if all others accepted the lie which the Party imposed—if all records told the same tale—then the lie passed into history and became truth. 'Who controls the past,' ran the Party slogan, 'controls the future: who controls the present controls the past.'"

- George Orwell, *1984*

93. In the wake of the 2020 presidential election and amidst a growing wave of public concern that the election results had been interfered with, tampered with, or manipulated to such a degree as to impact the outcome against Donald Trump and in favor of Joe Biden, Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") publicly claimed the 2020 election was the "most secure in American history." Dominion proudly touted that claim as vindication of its role in an election many claimed was stolen, and even continues to cite CISA's claim in support of its allegation that Mike Lindell's cries of election fraud are a "Big Lie." The real Big Lie is, in fact, CISA's claim that the 2020 election was the "most secure in American history."

94. For starters, what neither CISA nor Dominion nor Smartmatic bothered to tell the American people is that Dominion itself is a member of CISA's Election Infrastructure Sector Coordinating Council, and so wielded self-serving influence over CISA's proclamations that the 2020 election was historically unprecedented in its security. And, there is ample evidence that the 2020 presidential election was the furthest thing from secure—let alone "the most secure in American history."

95. On Monday, November 2, 2020, the night before the 2020 general 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."[67] Notably, Dominion had earlier *publicly denied* that any such updates just prior to election day were made and that its machines were connected to the internet—both of which were false statements.[68]

96. During the 2020 general 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.

97. 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.[69] Michael Spitzer-Rubenstein, a democrat political operative, was given internet access to a hidden Wi-Fi network at the Wisconsin election center where votes were being counted.[70]

---

[67] 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.

[68] https://www.theepochtimes.com/mkt_app/dominion-voting-machines-were-updated-before-election-georgia-official-confirms_3604668.html

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

[70] M.D. Kittle, *Democrats' Operative Got Secret Internet Connection at Wisconsin Election Center, Emails Show*, DAILY SIGNAL, Mar. 23, 2021, available at https://www.dailysignal.com/2021/03/23/democrats-operative-got-secret-internet-connection-at-wisconsin-election-center-emails-show/.

Spitzer-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.

98. 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 . . ."[71]

99. 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.[72] On January 27, 2021, the Maricopa County, Arizona Board of

[71] Oswego County, Index No. ECF 2020-1376, dated February 1, 2021 at 2.
[72] 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,

Supervisors voted unanimously to approve an audit of the 2020 election results and a forensic audit of Dominion's voting machines.[73] The Arizona senate hired a team of forensic auditors consisting of four companies to review Maricopa's election process.[74] A week later, attorneys sent each of those four companies a threatening cease-and-desist letter, improperly attempting to influence the reviews.[75] The audit began in April 2021 and, despite nearly-continuous efforts by left-minded litigants and certain Maricopa County officials to thwart it, is scheduled and on track to conclude on May 14, 2021.

b. In the Michigan case of *Bailey v. Antrim County*, 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.[76]

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/.

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

[74] Press Release, Arizona State Senate, Arizona Senate hires auditor to review 2020 election in Maricopa County (Mar. 31, 2021) (on file with author) (Ex. 10).

[75] 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. 11).

[76] 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).

c. In that same case, forensic analysts gained access to the Dominion voting machines used in the November 2020 election and determined the following:

   i. "The system intentionally generates an enormously high number of ballot errors … The intentional errors lead to bulk adjudication of ballots with no oversight, no transparency, and no audit trail."

   ii. "[T]he computer system shows vote adjudication logs for prior years; but all adjudication log entries for the 2020 election cycle are missing … Removal of these files violates state law."

   iii. "[A]ll'' server security logs prior to 11:03 pm on November 4, 2020 are missing. This means that all security logs for the day after the election, on election day, and prior to election day are gone … Other server logs before November 4, 2020 are present; therefore, there is no reasonable explanation for the security logs to be missing." [77]

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

[77] Allied Security Operations Group Revised Preliminary Summary v.2, Antrim Michigan Forensics Report, 12/13/2020, available at https://www.depernolaw.com/uploads/2/7/0/2/27029178/ex_8-9.pdf.

e. On March 23, 2020 the Wisconsin Assembly ordered an investigation into the 2020 election. Wisconsin uses Dominion voting machines.[78]

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

Even the Biden administration has recently sanctioned Russia for election interference and hacking.[79]

100. In early 2021, a data scientist, Douglas G. Frank, PhD, uncovered an algorithm or "key"—a sixth degree polynomial—that operates in the electronic voting machines in a number of states to determine the ballots cast. These algorithms are unique to each particular state. In other words, the algorithm used in Minnesota does not work next door in Wisconsin. Likewise, the algorithm in Ohio does not work in Michigan or in Pennsylvania. That fact further demonstates an algorithm is at work and the voter results are not random. Each algorithm is determined at the state level to shift votes based on the particular and peculiar demographics of each state. The examples below are from counties in Minnesota, but Dr. Frank has done the same analysis in a number of other states, including Michigan, Ohio, Pennsylvania, North Carolina, Washington, Colorado, and Florida, and reached the same results and conclusions.

---

[78] 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.

[79] *See, e.g.*, Truak, Natasha and Amanda Macias, "Biden administration slaps new sanctions on Russia for cyberattacks, election interference," Apr. 14, 2021, https://www.cnbc.com/2021/04/15/biden-administration-sanctions-russia-for-cyber-attacks-election-interference.html.

101. Specifically, the algorithm is a mathematical computation of the actual registrations compared to the actual ballots cast. When applied to the 2019 census data and the registration data, that algorithm enables the prediction of the number of ballots cast *for each voter age group* in any given county in a state with near 100% certainty—without seeing the actual results. The key for each state applies with 100% certainty or near 100% certainty for every county within that state. And, as stated above, each state has a unique key. That does not happen in a random world.

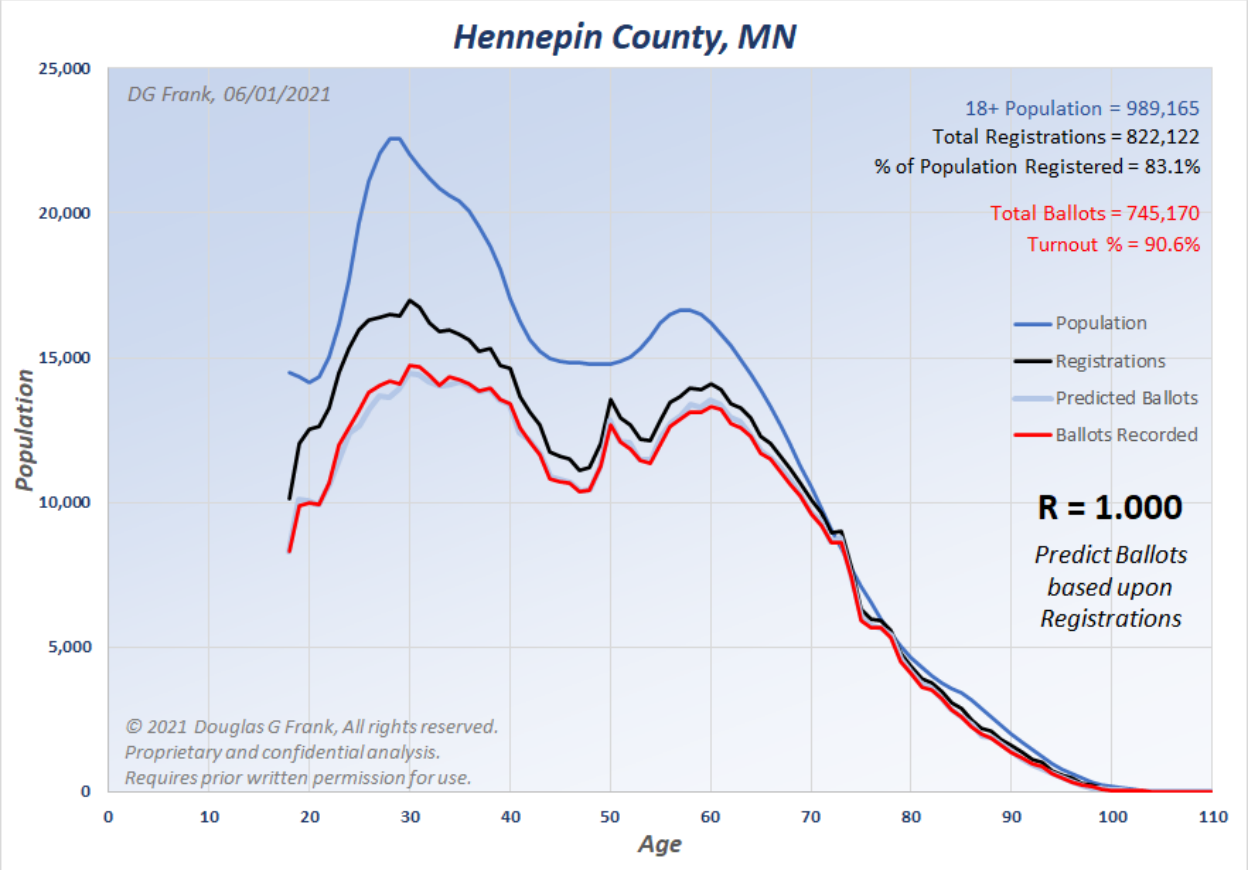
102. Specifically, with respect to the charts for the respective Minnesota counties below:

a. The data is shown in graphs and compiled from three different databases:

BLUE CURVE. Population data extracted from the 2019 U.S. census at census.gov. This is the blue curve on each chart for the counties examined, which shows the census data per age group.

BLACK LINE. The state registration database for used in the November 3, 2020 election. This is the black line on each chart.

RED LINE. The state voter database with recorded results after the election. This is the red line on each chart.



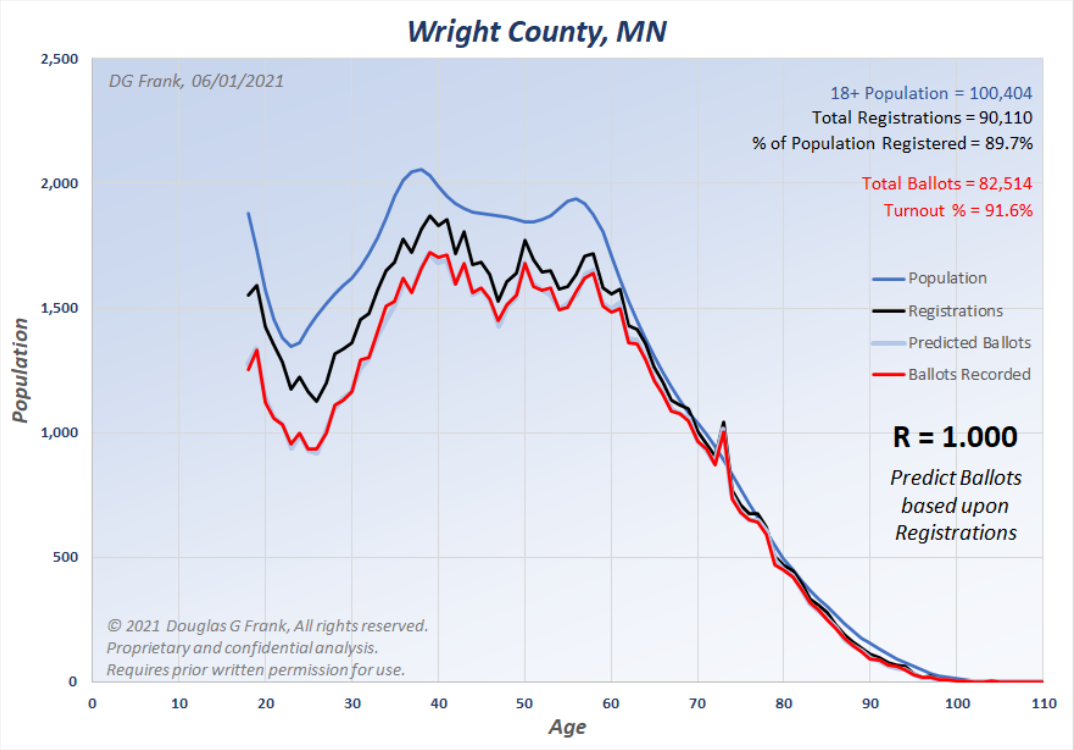
b. The blue, black, and red lines on the graphs are data. They are not speculative or calculated. The are comprised of 100% data. The algorithm itself, a sixth degree polynomial, is a mathematical computation of the actual registrations on each graph (black line) compared to the actual ballots cast (red line). The polynomial can be described as a "key" because it works in every county in a state e.g. Minnesota. The algorithm is regulating voter turnout by age as shown by the fact that voter turnout by age is in the exact same relative proportion to registered voters in each county in any given state. What happens in one county happens in all counties in a given state. The almost-

perfect correlation also means that by taking the census data and the registration data and then applying the algorithm, the number of ballots cast in a county can be predicted with virtually perfect certainty without even seeing the results.

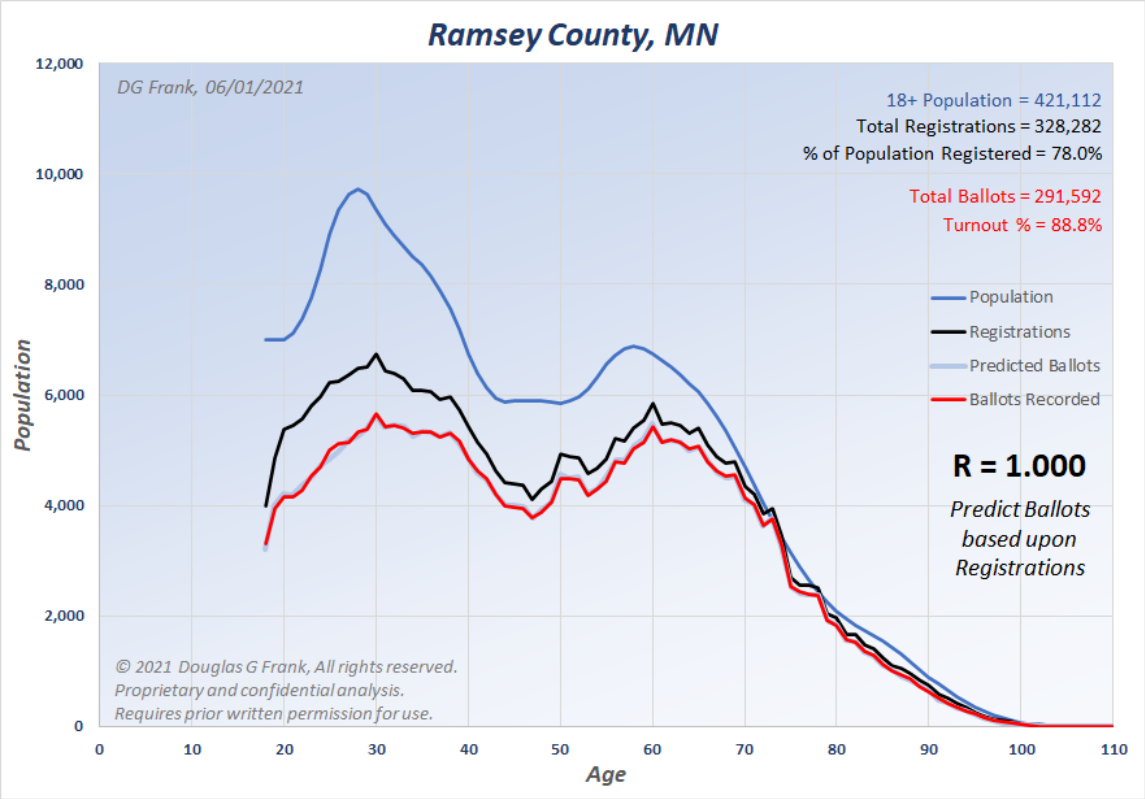
c. To discover the key, Dr. Frank first charted the total voting population that could be registered (dark blue line). Dr. Frank then layered in the registered voters (black line). Next, Dr. Frank included the actual ballots cast (red line). When all of the bumps in the black line (registrations) are compared to those in the red line (ballots), they look very familiar. The red line is almost a direct image of the black line, but just lower on the graph. Simply graphing the ratio between the black and the red creates the polynomial. The polynomial becomes the key. The key is then used and works in every county in a given state. When the key is applied, it generates the light blue line (predicted ballots).

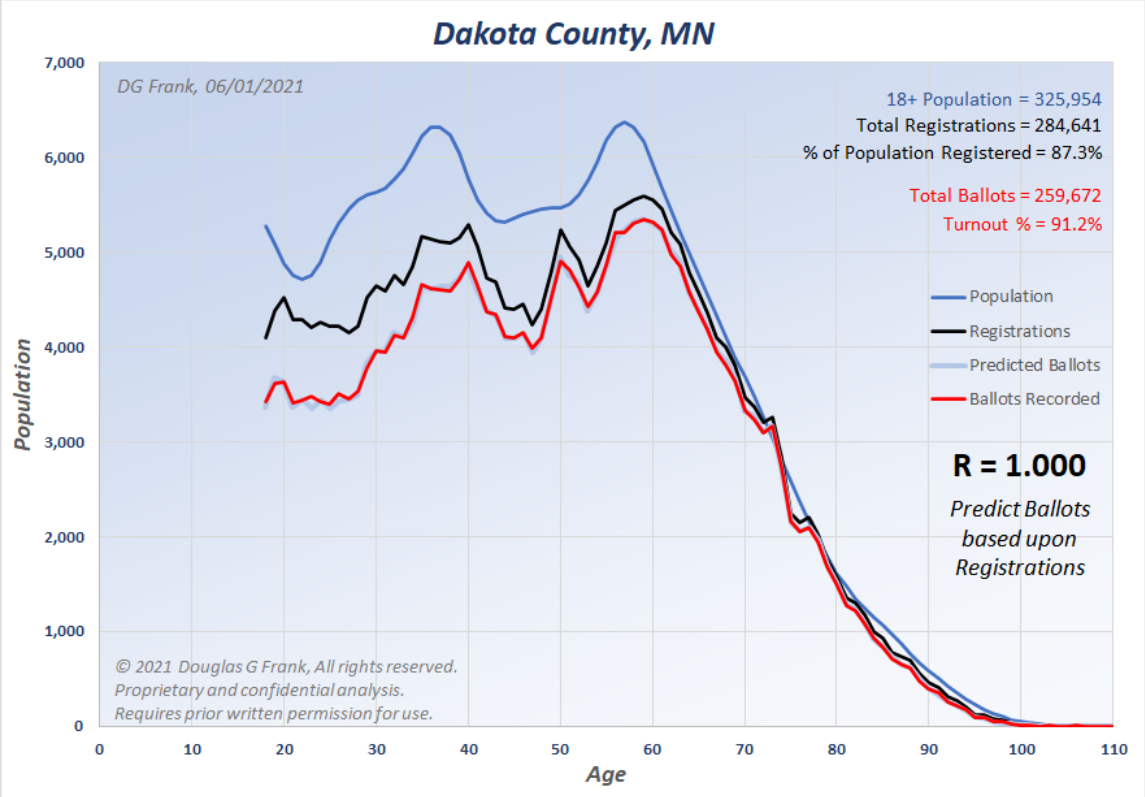
d. Dr. Frank applied the algorithm (a sixth degree polynomial) and predicted the number of ballots cast per age group in each county. This is represented by the light blue line (predicted ballots). The red line (actual ballots cast) tracks almost identically with the ballots predicted by the key. The light blue line (predicted ballots, using the "key") also tracks with the black line (registrations). Those curves also follow the shape of the census (*i.e.,* the population).

e. As found for several other states, in Minnesota, Dr. Frank's algorithm consistently predicted voter participation demographics to remarkably unnatural precision, with nearly every correlation coefficient equal or greater than 0.990. In Minnesota alone, he predicted 13 counties with R = 1.000, 33 counties with R = 0.999, 22 counties with R = 0.998, and all the rest greater than 0.994 except for three, the worst of which was R = 0.976—still impossibly high to be a random event.[80] Three such counties are depicted in the charts below:



[80] All of the county charts can be viewed at https://www.youtube.com/watch?v=xkY2LRA1ijQ


Ramsey County, MN
DG Frank, 06/01/2021
18+ Population = 421,112
Total Registrations = 328,282
% of Population Registered = 78.0%
Total Ballots = 291,592
Turnout % = 88.8%
Population
Registrations
Predicted Ballots
Ballots Recorded
R = 1.000
Predict Ballots based upon Registrations
© 2021 Douglas G Frank, All rights reserved.
Proprietary and confidential analysis.
Requires prior written permission for use.
Population
Age
12,000
10,000
8,000
6,000
4,000
2,000
0
0
10
20
30
40
50
60
70
80
90
100
110


Dakota County, MN
DG Frank, 06/01/2021
18+ Population = 325,954
Total Registrations = 284,641
% of Population Registered = 87.3%
Total Ballots = 259,672
Turnout % = 91.2%
Population
Registrations
Predicted Ballots
Ballots Recorded
R = 1.000
Predict Ballots based upon Registrations
© 2021 Douglas G Frank, All rights reserved.
Proprietary and confidential analysis.
Requires prior written permission for use.
Population
Age
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
0
10
20
30
40
50
60
70
80
90
100
110

f. The analysis of the data shows an ability to predict ballot demographics with a degree of precision approaching 100%—a level of accuracy that would be impossible without the activity of a regulating algorithm. And, the degree of precision observed confirms that algorithms had real-time access to voting databases and voting activity before, during, and following the November 3, 2020 election.

103. Dr. Frank also found such a key in all 88 counties in Ohio, all 64 counties in Colorado, in all 14 counties evaluated in Florida, and in all 14 counties evaluated in Pennsylvania. Elections should not function like this in a normal statistical way. That is why Dr. Frank concludes that someone is deciding what this key is before the election and then making every county fit this key. And the key is able to be used to determine elections because the electronic voting machines are computers—computers highly vulnerable to hacking, tampering, and cyberattacks.[81]

104. In addition, Exhibit 12 showsa subset of 20 documented successful hacks through the election management system in the states of Michigan, Pennsylvania, Georgia, Wiscinsin, and Arizona resulting in a total 555,864 votes switched from President Trump to candidate Vice President Biden in the 2020 general election. These hacks came primarily from within China and are identified by the date, location, and the network from which the hack orginated and the location and network that was the target of the hack. The network

[81] Dr. Frank's analysis for these states (and others) is viewable at https://www.youtube.com/channel/UC57eE4MaR0oIwTinM__WQSg.

packets of information flowing from these hacks was capturedand recorded in real time as discussed in the documentary, "Absolute 9-0."[82]

105. In short, every mainstream media "reporter" and social media pundit continues to label the fact of tampering and interference in the 2020 election as "baseless," "false," "debunked," or some similarly approved newspeak. But "baseless," "false," "debunked," and similar adjectives are not synonyms for "disputed." The media and big-tech orthodoxy may *dispute* the sources, methodologies, or conclusions that lead many to question the 2020 election, but they are beyond disingenuous to claim such questions have no basis or have been conclusively or objectively answered in favor of their view. They are ignoring the cacophony of complaints from the political left prior to November 3, 2020. And they are literally asking Americans to ignore open and obvious evidence—evidence of events *they themselves predicted would occur*—and instead yield meekly to their campaign of enforced doublethink.

E. Shut Up Or Else

"Being in a minority, even a minority of one, did not make you mad. There was truth and there was untruth, and if you clung to the truth even against the whole world, you were not mad."

- George Orwell, *1984*

106. Lindell has spoken out personally about Dominion, about electronic voting machines more generally, and the importance of election integrity. And, Lindell has spoken accurately about these issues of great public concern. He has presented evidence backed

[82] *See* https://www.worldviewweekend.com/tv/video/mike-lindell-presents-absolutely-9-0, beginning of the documentary through the 16 minute mark.

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.[83]

107. However, Dominion's true purpose is not simply to silence Lindell, but to silence anyone else who might speak out on election fraud. Thus, Dominion also sued the company Mike Lindell founded and owns. MyPillow made no statements about Dominion. Instead, by suing MyPillow, Dominion seeks to punish Lindell for *his* statements by damaging his reputation, his finances, and his business. More fundamentally, Dominion—in cohoots with Smartmatic—also seeks to send a message to others: "Shut up or else."

108. That is why Dominion's campaign also included bragging publicly about having its lawyers at Clare Locke send threatening letters to over 150 individuals demanding they cease and desist from commenting on the election or Dominion.[84] Among the recipients of these shotgun-style attack letters are dozens of 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

[83] *See* Case No. 1:21-cv-00445-CJN; *US Dominion, Inc., et al. v. My Pillow, Inc. and Michael J. Lindell*; in the United States District Court for the District of Columbia ("the D.C. Lawsuit").

[84] Hannah Knowles and Emma Brown, *Dominion threatens MyPillow CEO Mike Lindell with lawsuit over 'false and conspiratorial' claims*, Washington Post, Jan. 18, 2021, https://www.washingtonpost.com/politics/2021/01/18/dominion-mike-lindell-mypillow/.

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 Clare Locke's threats constitute witness intimidation.

109. However, Dominion did not stop there. To give its letters further intimidating weight, Dominion's public campaign extended to suing 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 blitz 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.

110. Through aggressive litigation, threats of litigation, and publicization of these activities, Dominion seeks to intimidate those who might dare to come forward with evidence of election fraud, 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.

111. 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.[85] 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.

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

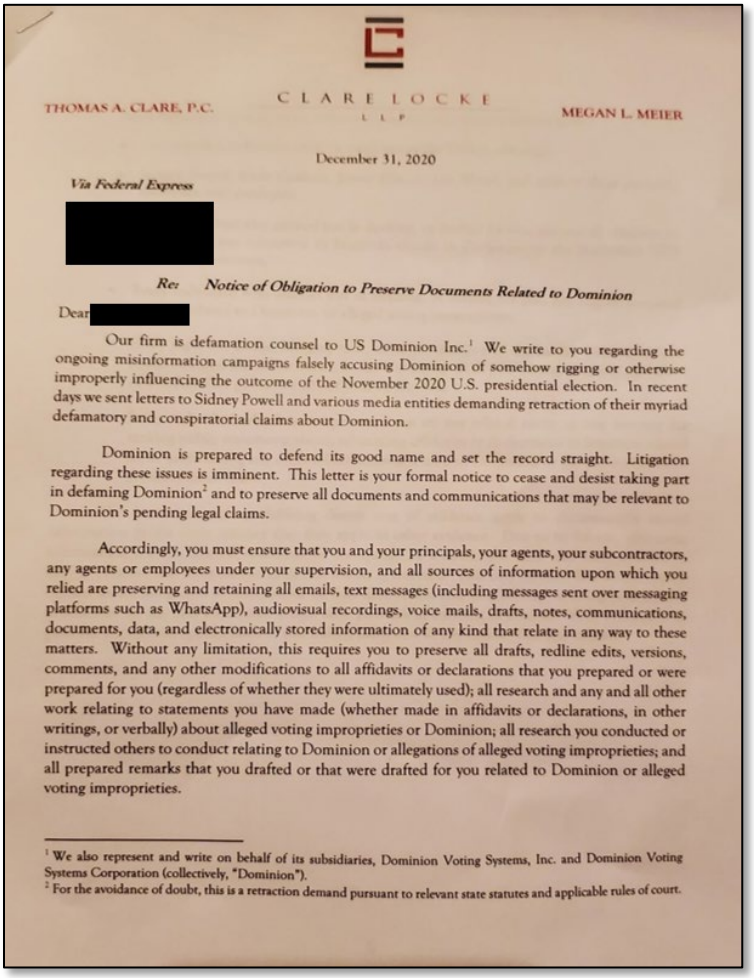
a. Dominion has sent at least 150 attorney letters, threatening the recipients with legal action. Some of these letters include copies of Dominion's legal papers in its lawsuits. The clear message of these letters is that anyone who comments publicly about Dominion will be ruined.

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* questioning 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. Exhibits 13 and 14 are representative of the

[85] "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.

threatening letters Dominion and Clare Locke sent to dozens of these citizen volunteers performing a public service.

c. In another 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 cease and desist letter. As a result of speaking out, the actuary lost business.

113. 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."

114. 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.

115. 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.

116. 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 his company. Exhibits 15 through 17 are the increasingly aggressive "cease and desist" letters sent by Dominion's lawyers at Clare Locke to Lindell, seeking to silence Lindell's criticism and cherry-pick support for Dominion's self-interested denial of any wrongdoing. Dominion's and Smartmatic's scheme is wrongful because their purpose is to punish and deter important constitutionally-protected activity–free expression about a matter of public concern.

117. Dominion's co-conspirator in this campaign to suppress free speech and extort silence from dissenters is another election-runner and state actor, Smartmatic. On or about February 4, 2021, Smartmatic filed a *$2.7 billion* lawsuit in federal court in New York City against Fox News; journalists Lou Dobbs, Maria Bartiromo, and Jeanine Pirro; and former Trump attorneys Rudy Giuliani and Sydney Powell. The defendants' alleged wrongdoing? Speaking their mind publicly, attempting to report on growing questions about the role of voting machines in 2020 election irregularities, and utilizing the legal process to expose such irregularities and prevent certification of any election results that may have resulted from a tainted process. But Smartmatic's true motive is as obvious as Dominion's: to enforce the orthodoxy of Democrats, the mainstream media, and Big Tech

and quash any and all suggestions that President Joe Biden might not have been the victor in an election conducted fairly and untainted by fraud. And Smartmatic's weapon of choice? The litigation process—an expensive, slow, notoriously inefficient arena in which only a very few can afford to wage battle on the scale Smartmatic and Dominion attempt to impose on those who question the integrity of their systems. Under the auspices of "defending election integrity"—a lofty goal far better served by fixing their notoriously and demonstrably insecure voting machines than by waging lawsuit warfare on private citizens—Smartmatic and Dominion have embarked on a concerted, collective enterprise to extort silence from their dissenters or bring financial ruin on any and all who persist in speaking their minds.[86]

118. Lindell is a victim of this conspiracy and enterprise by Dominion and Smartmatic to attempt to silence him by abusing the litigation process and, as state actors, punish him for his support and advocacy of certain political views or candidates. Specifically, he has suffered reputational harm from being called the perpetrator of the "Big Lie"—a Hitler-coined term[87]—and publicly vilified as a liar, conspiracy theorist, and purveyor of "basless" or "false" information regarding the 2020 election. Moreover, Lindell has received numerous threats against his person and even his life since speaking out about evidence of election fraud. Obviously, he has suffered individually as a result of the damage done to his business, MyPillow, as a result of the Dominion- and Smartmatic-

[86] https://www.businessinsider.com/everyone-dominion-smartmatic-suing-defamation-election-conspiracy-theories-2021-2

[87] ADOLF HITLER, MEIN KAMPF vol. I, ch. X (James Murphy trans., Hurst and Blackett Ltd. 1939) (1925) available at http://gutenberg.net.au/ebooks02/0200601.txt.

led "cancel culture" aimed at Lindell. And the Dominion lawfare campaign against Lindell has interfered with plans to take Lindell's on-line store, MyStore, public in an initial public offering. Moreover, he has incurred and is incurring hundreds of thousands of dollars to defend himself against Dominion's $1.3 billion lawsuit simply because Dominion wants to use the litigation process to silence him—even as it tolerated a decade or more of criticism of its machines' security from those on the political left. Lindell is entitled to recover his actual and special damages from Dominion and Smartmatic for their collective role in their conspiracy and enterprise to harm him—damages which presently are estimated to exceed $2 billion.

119. In the context of election integrity—so crucial to the functioning and survival of a republican form of government—no litigant should be able to weaponize the courts and the litigation process while hiding behind legal doctrines originally intended and developed to *protect* constitutional rights, such as the right to petition the government, and the right to a full and fair opportunity to be heard in a court of law. No doubt, the Dominion Defendants and the Smartmatic Defendants will attempt to hide behind such doctrines (like the *Noerr-Pennington* doctrine or the "absolute privilege" protecting statements made in the course of judicial proceedings) to *deprive* Lindell and other litigants of their sacrosanct right of freedom of speech. Through their joint enterprise to suppress political dissent, the Dominion Defendants and the Smartmatic Defendants have placed in tension the right to petition the government against the right to free speech. In doing so, one set of litigants (the Dominion and Smartmatic Defendants) have abused the right to petition the government in an effort to suppress Mike Lindell's and others' lawful and proper exercise

of their freedom of speech. Plaintiff Lindell has been harmed as a result and brings this suit to recover for that harm and bring an end once and for all to the defendants' reign of litigation terror and conspiracy to deprive Lindell and others of their constitutionally protected freedom of political expression.

120. In short, Plaintiff Lindell brings this lawsuit to put an end to Dominion's and Smartmatics' campaign of "lawfare" against those who criticize their electronic voting machines, or who question their role in the indisputably suspect conduct of the 2020 President Election. Lindell's claims rise above any protections the defendants may assert to wage their lawfare campaign, because those protections do not and should not immunize state actors from weaponizing the judicial system and the litigation process to silence dissent, unpopular beliefs, or facts inconveniently out-of-line with mainstream groupthink.

VI. CAUSES OF ACTION

"Freedom is the freedom to say that two plus two make four. If that is granted, all else follows."

- George Orwell, *1984*

121. The facts alleged above and to be proven at trial demonstrate that Plaintiff is entitled to recover damages and other relief against the various defendants in this case on one or more theories and causes of action as set out below.

COUNT ONE: ABUSE OF PROCESS
(as to the Dominion Defendants)

122. Plaintiff incorporates the foregoing paragraphs as if fully set forth verbatim below.

123. The facts set forth herein and to be proven at trial demonstrate that Plaintiff is entitled to recovery against the Dominion Defendants, jointly and severally, for the common law tort of abuse of process.

124. Under Minnesota law, the elements of a tort cause of action for abuse of process are (a) the existence of an ulterior purpose, and (b) the act of using the process to accomplish a result not within the scope of the proceeding in which it was issued, whether such result might otherwise be lawfully obtained or not. *See Young v. Klass*, 776 F.Supp.2d 916, 924 (D. Minn. 2011), *quoting Hoppe v. Klapperich*, 224 Minn. 224, 28 N.W.2d 780, 786 (1947). Abuse of process does not require the plaintiff to prove either favorable termination of the underlying litigation or malice on the part of the defendant.

125. The facts alleged above and to be proven at trial will establish each of these elements. As detailed above, the Dominion Defendants brought suit against Lindell as part of a widespread "lawfare" campaign designed not to compensate for any harm to Dominion caused by the public statements by Lindell and others, but to weaponize the judicial system in order to quash political dissent and silence those who would have the citizens of the United States (and the world, for that matter) know the truth about the grave flaws in Dominion's voting machines (as well as the voting machines of others). To that end, the Dominion Defendants have willfully plead gross mischaracterizations and outright lies about their voting machines, about the public statements Lindell has made about them, and about Lindell personally. In addition, the Dominion Defendants have alleged a quantum of damages—$1.3 *billion*—that not only bears no conceivable connection to any possible harm suffered from the public exposé of their flawed machines, but also is many multiples

of the Dominion Defendants' revenues from their voting machines that were the subject of Lindell's public statements. Such allegations, having no basis in fact, are instead meant only to intimidate and silence. For these and other reasons, the Dominion Defendants' judicial claims against Lindell are devoid of factual support and were instead made for the primary purpose of intimidating Lindell into silence and a public retraction of his previous public statements.

126. As a result of the Dominion Defendants' abuse of the judicial process, Plaintiff has suffered damages to his business interests and his reputation, has suffered threats to his personal safety and life, and has incurred and continues to incur costs to defend the abusive litigation those defendants have brought against him, for which he is entitled to recovery against those defendants, jointly and severally, and for which he now brings this suit.

COUNT TWO: DEFAMATION
(as to the Dominion Defendants)

127. Plaintiff incorporates the foregoing paragraphs as if fully set forth verbatim below.

128. Pleading further and in the alternative, the facts set forth herein and to be proven at trial demonstrate that Plaintiff is entitled to recovery against the Dominion Defendants, jointly and severally, for the common law tort of defamation.

129. Under Minnesota law, a statement is actionable in defamation if it is: (1) false; (2) was communicated to a third party; and (3) tended to harm the plaintiff's reputation or to lower that person in the estimation of the community. *Church v. City of*

St. Michael, 205 F.Supp.3d 1014, 1043 (D. Minn. 2016). Defamation that affects a plaintiff in its "business, trade, profession, office or calling" is defamation per se and is "actionable without any proof of actual damages." *Id.* at 1045 n.19.

130. The Dominion Defendants have defamed Plaintiff Lindell *per se* by calling him a "liar" and a purveyor of "the Big Lie" in the D.C. Lawsuit. In fact, everything Lindell has publicly stated about the vulnerability of voting machines to cyberattacks and hacking (including the Dominion Defendants' voting machines) is substantively true, and the Dominion Defendants know it.

131. Labeling a private citizen a "liar" or purveyor of lies is defamation *per se*, and therefore Lindell is entitled to monetary relief even in the absence of proof of economic loss or special damages. To the extent such proof is required, Plaintiff will show that the Dominion Defendants' published lies about him have caused him economic losses and special damages, for which he is entitled to recovery against those defendants, jointly and severally, and for which he now brings this suit.

COUNT THREE: VIOLATIONS OF THE RACKETEER INFLUENCED AND CORRUPT ORGANIZATION ACT, 18 U.S.C. § 1962
(as to Dominion Defendants and Smartmatic Defendants)

132. Plaintiff incorporates the foregoing paragraphs as if fully set forth verbatim below.

133. Pleading further and in the alternative, the facts set forth herein and to be proven at trial demonstrate that Plaintiff is entitled to recovery under 18 U.S.C. § 1964

against the Dominion Defendants and the Smartmatic Defendants, jointly and severally, for violations of the Racketeer Influenced and Corrupt Organization Act, 18 U.S.C. § 1962.

134. To establish a civil RICO claim, the plaintiff must show that the defendant engaged in (1) conduct (2) of an enterprise (3) through a pattern (4) of racketeering activity, and that he (5) sustained an injury to business or property (6) that was caused by the RICO violation.

135. An "enterprise" includes any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity. An "association-in-fact" enterprise does not require a formal structure such as a hierarchical chain-of-command, fixed roles for members, a name, regular meetings, or established rules and regulations. To establish an enterprise, the plaintiff must show (1) a common purpose, (2) relationships among those associated with the enterprise, and (3) longevity sufficient to permit those associates to pursue the enterprise's purpose.

136. The facts alleged above and to be proven at trial demonstrate that the Dominion Defendants and the Smartmatic Defendants, with the assistance and participation of non-party co-conspirator Clare Locke, LLP, constituted an association-in-fact enterprise ("the Dominion/Smartmatic Enterprise") having the common purpose of suppressing dissent to the use of electronic voting machines and suppressing demands for investigations into the possible use of electronic voting machines to artificially manipulate voting, vote tabulations, and election results reporting in the 2020 Presidential Election. A relationship exists between the Dominion Defendants and the Smartmatic Defendants in

that the Dominion Defendants' voting machines utilize Smartmatic software (or software previously designed, created, modified, and sold by Smartmatic), and the Dominion Defendants and Smartmatic Defendants share common employees or contractors, co-working space, and historical and functional connections to Sequoia and other legacy voting systems. This relationship has existed for over ten years and continues to this day.

137. The facts alleged above and to be proven at trial demonstrate that the Dominion/Smartmatic Enterprise was at all relevant times engaged in the production, distribution, or acquisition of goods or services in interstate commerce. Specifically, the Dominion Defendants' principal place of business is in Colorado, but Dominion provides voting machines to twenty-eight different states, and has issued written threats to those speaking out against electronic voting machines and their vulnerability to vote manipulation in numerous states beyond the borders of the State of Colorado, and has filed suit against Plaintiff Lindell in the District of Columbia as part of the "lawfare" campaign of the Dominion/Smartmatic Enterprise. Likewise, Smartmatic has its principal place of business in Florida, but has likewise sold its goods and services—which it too seeks to protect through the joint "lawfare" campaign as part of the Dominion/Smartmatic Enterprise—to numerous jurisdictions outside of Florida and throughout the United States.

138. The facts alleged above and to be proven at trial further demonstrate that the Dominion/Smartmatic Enterprise has engaged in numerous related acts of racketeering activity that amount to or pose a threat of continued criminal activity. Specifically, the Dominion/Smartmatic Enterprise has issued—according to Dominion's own boasting on its website—over 150 "cease and desist" letters threatening companies and individuals

(including family members of those who have spoken publicly against the voting machines, who have not themselves spoken publicly about them). Those letters threaten the recipients with ruinous litigation unless the recipients recant their previous statements and cease further public expression regarding questions or evidence of fraudulent manipulation of voting machines or their use in tampering with and altering the outcome of the 2020 Presidential Election in certain jurisdictions. These threats constitute extortion for purposes of establishing the requisite "predicate acts" for a civil RICO claim. These threats constitute a "pattern" for purposes of a civil RICO claim because the Dominion/Smartmatic Enterprise has made them continuously since shortly after the 2020 Presidential Election, and it continues to issue new extortionate threats to additional recipients to this day, with no apparent end in sight to the pattern of racketeering activity.

139. Plaintiff has suffered actual injury as a result of the Dominion/Smartmatic Enterprise's actions in furtherance of its racketeering conspiracy and activities, for which he is entitled to recovery against those defendants, jointly and severally, together with treble damages as allowed by law, as well as attorney's fees, and for which he now brings this suit.

COUNT FOUR: VIOLATIONS OF THE "SUPPORT AND ADVOCACY" CLAUSE OF 42 U.S.C. § 1985(3)
(as to Dominion Defendants and Smartmatic Defendants)

140. Plaintiff incorporates the foregoing paragraphs as if fully set forth verbatim below.

141. Pleading further and in the alternative, the facts set forth herein and to be proven at trial demonstrate that Plaintiff is entitled to recovery under 42 U.S.C. § 1985(3) against the Dominion Defendants and Smartmatic Defendants, jointly and severally, for violation of Plaintiff's rights under the Support and Advocacy clause of that statute.

142. The "Support and Advocacy" clause of 42 U.S.C. § 1985(3) provides as follows:

> [I]f two or more persons conspire to prevent by force, intimidation, or threat, any citizen who is lawfully entitled to vote, from giving his support or advocacy in a legal manner, toward or in favor or the election of any lawfully qualified person as an elector for President or Vice President …; or to injure any citizen in person or property on account of such support or advocacy; … if any one or more persons engaged therein do, or cause to be done, any act in furtherance of the object of such conspiracy, whereby another is injured in his person or property, or deprived of having and exercising any right or privilege of a citizen of the United States, the party so injured or deprived shall have an action for the recovery of damages occasioned by such injury or deprivation, against any one or more of the conspirators.

Id.

143. A cause of action under the Support and Advocacy clause therefore requires a showing of the following elements: (1) two or more persons; (2) who conspire to either (a) prevent by force, intimidation, or threat a citizen lawfully entitled to vote from giving support or advocacy in a legal manner toward or in favor of the election of a lawfully qualified elector for President or Vice President, or (b) injure any citizen in person or property on account of her support or advocacy toward or in favor of the election of a lawfully qualified elector for President or Vice President; (3) one or more acts in furtherance of the object of such conspiracy; (4) whereby plaintiff suffers either (a) injury in her person or property, or (b) deprivation of having and exercising any right or privilege

of a citizen of the United States. *Id.*; *see also*, Note, "The Support and Advocacy Clause of § 1985(3), HARVARD LAW REVIEW 133:1382, 1384-86 (2020).

144. The facts set out above and to be proven at trial demonstrate that the Dominion Defendants and the Smartmatic Defendants, with the assistance and participation of non-party co-conspirator Clare Locke, LLP, had a meeting of the minds to agree on the common purpose of silencing dissent and opposition to the use of electronic voting machines in the 2020 Presidential Election and the exposure of such machines' vulnerability to cyber attacks and election tampering. The real purpose of the conspiracy was to silence those like Lindell who supported President Donald J. Trump and advocated for investigations into voting machine fraud (and other types of election fraud) in an effort to determine the legitimate votes cast for each Presidential candidate in each of the key swing states, in light of the numerically improbable overnight lead change from Trump to Biden in those states in the wee hours of November 4, 2020. The Dominion Defendants and the Smartmatic Defendants determined to carry out this conspiracy through a coordinated campaign of lawfare—weaponizing the court system and litigation process to threaten, intimidate, and force private citizens like Lindell into silence and retract their public statements regarding opposition to the use of electronic voting machines and their vulnerabilities, and the significant potential that such vulnerabilities were exploited in certain jurisdictions to artificially cost President Trump the election in key swing states. To that end, the Dominion Defendants first threatened Lindell with ruinous litigation, then filed an abusive, sham defamation lawsuit against Lindell seeking a $1.3 *billion* recovery with no basis in fact or law. The Dominion Defendants' lawsuit has injured Lindell in his

person (reputationally and physically due to threats on his life) and his property (through business losses and the cost of defending against the sham litigation) and has further deprived Lindell of having and exercising his rights as a United States citizen to freedoms of speech and of expression.

145. The Dominion and Smartmatic Defendants' violation of the Support and Advocacy clause of 42 U.S.C. § 1985(3) has caused Plaintiff Lindell actual damages, for which he is entitled to recovery against those defendants, jointly and severally, and for which he now brings this suit.

146. Separately, a conspiracy for purposes of this claim is shown by the actions of the Dominion Defendants and their lawyers at Clare Locke, LLP who together conspired to send out over 150 baseless cease and desist letters—including to Lindell—with the express purpose of threatening and intimidating Lindell and others who brought forth evidence of election fraud in the November 2020 general election as part of their support and advocacy for President Trump.

COUNT FIVE: 42 U.S.C. § 1983 DEPRIVATION OF CIVIL RIGHTS BY ACTIONS UNDER COLOR OF STATE LAW
(as to Dominion Defendants)

147. Plaintiff incorporates the foregoing paragraphs as if fully set forth verbatim below.

148. Pleading further and in the alternative, the facts set forth herein and to be proven at trial demonstrate that Plaintiff is entitled to recovery under 42 U.S.C. § 1983

against the Dominion Defendants, jointly and severally, for violation of Plaintiff's rights under the Equal Protection Clause of the United States Constitution and under the Due Process Clause of the Fifth and Fourteenth Amendments to the United States Constitution.

149. The Dominion Defendants were at all relevant times acting under color of state law in connection with the 2020 Presidential Election. Specifically, a private party is acting under color of state law when the state has delegated to that private party a function traditionally exclusively reserved to the State. Administering elections of public officials is one such function, and the facts alleged above and to be proven at trial will demonstrate that the Dominion Defendants were administering elections in numerous jurisdictions throughout and across the United States, the results of whose local 2020 presidential voting significantly and materially impacted the outcome of the 2020 Presidential Election nationally.

150. To establish a Section 1983 claim, a plaintiff must show that (1) he has Article III standing to bring the claim, (2) a right secured by the Constitution or laws of the United States was violated, and (3) the alleged violation was committed by a person acting under the color of state law. *Parratt v. Taylor,* 451 U.S. 527, 535 (1981), *overruled in part on other grounds* by *Daniels v. Williams,* 474 U.S. 327, 330–31 (1986).

151. To establish a violation of the Equal Protection Clause under 42 U.S.C. § 1983, the plaintiff must show state action that inherently favors or disfavors a particular group of voters. The facts alleged above and to be proven at trial will demonstrate that the Dominion Defendants acted under color of state law to engage in invidious discrimination or intentional misconduct to the detriment of Lindell and others of his same class of voter.

Specifically, the Dominion Defendants, acting under color of state law as a private corporation authorized and employed by various states to perform the essential state function of administering and conducting the 2020 Presidential Election, have attempted through the use of the courts and the litigation process to suppress Lindell's freedom of speech and his right to disseminate information and data regarding the role of Dominion voting machines in election fraud and election tampering. In doing so, Dominion disfavored the conservative political viewpoint of Plaintiff Lindell over those of left-leaning or Democrat-supporting individuals *who also publicized the role of Dominion voting machines in election fraud and election tampering.* A state actor like the Dominion Defendants cannot engage in viewpoint-based discrimination in attempting to suppress a private citizen's exercise of its First Amendment right to free speech, and in doing so, the Dominion Defendants unlawfully deprived Plaintiff Lindell of a legally protected interest in violation of 42 U.S.C. § 1983.

152. To establish a substantive due process violation under 42 U.S.C. § 1983, the plaintiff must demonstrate that a fundamental right was violated and that the conduct shocks the conscience. Freedom of speech—and in particular, freedom of political speech—is, indisputably, a right of the most fundamental significance under our constitutional structure. The facts alleged above and to be proven at trial will demonstrate that the Dominion Defendants acted under color of state law to engage in conduct that shocks the conscious because it was so disproportionate to the need presented, and so inspired by malice or sadism rather than a merely careless or unwise excess of zeal, that it amounted to brutal and inhumane abuse of official power literally shocking to the

conscience. Specifically, the Dominion Defendants, acting under color of state law, misused the courts and the litigation process to suppress Lindell's freedom of speech and to deprive him of a substantive right under the First Amendment. Such wrongdoing violates 42 U.S.C. §1983 and has caused Plaintiff Lindell harm, for which he now brings this suit.

COUNT SIX: CIVIL CONSPIRACY
(as to All Defendants)

153. Plaintiff incorporates the foregoing paragraphs as if fully set forth verbatim below.

154. Pleading further and in the alternative, the facts set forth herein and to be proven at trial demonstrate that Plaintiff is entitled to recovery for common law civil conspiracy against all Defendants, jointly and severally, for their collusion and agreement to the common objective or course of action, acting under color of state law, to deprive Plaintiff Lindell of his constitutional rights under the First Amendment, and their overt acts in connection with that common purpose.

155. To establish a civil conspiracy, plaintiffs must show five elements: (1) two or more persons; (2) an object to be accomplished; (3) a meeting of the minds on the object or course of action to be taken; (4) the commission of one or more unlawful overt acts; and (5) damages as the proximate result of the conspiracy. *See ECTG Ltd., Trustwater, Ltd. v. O'Shaughnessy*, No. CIV. 14-960 DSD/JJK, 2014 WL 6684982, at *4 (D. Minn. Nov. 25, 2014), *citing In re TMJ Implants Prods. Liab. Litig.,* 113 F.3d 1484, 1498 (8th Cir.1997).

156. The facts set out above and to be proven at trial will establish that Defendants collectively, with the assistance and participation of non-party co-conspirator Clare Locke, LLP, had a meeting of the minds on the object or course of action of depriving Plaintiff of his constitutional rights under the First Amendment, while acting under color of state law. The facts will further establish that Defendants committed one or more wrongful overt acts, including but not limited to the following, in furtherance of this common objective or course of action:

a. Engaging in a campaign of abuse of process to bring suit against Plaintiff not for the purpose of vindicating any legitimate right or grievance but for the sole purposes of intimidating Lindell into silencing his political speech and opposition to Defendants' point of view.

b. Defaming Plaintiff by publishing false and defamatory statements, including but not limited to calling him a "liar" and the purveyor of "the Big Lie," when Defendants were aware that Plaintiff's statements were substantively true.

c. Attempting to extort Plaintiff by first threatening him with ruinous litigation, then actually bringing such litigation in a sham or frivolous manner, if he refused to silence his views on the reliability of voting machines and their use to alter election outcomes in certain jurisdictions, or to retract his prior statements to that effect.

d. Violating Plaintiff's rights under the "Support and Advocacy" clause of 42 U.S.C. § 1985(3) by attempting first to intimidate him into silencing his political speech, then punishing him for continuing to exercise his right to

speak, regarding the vulnerability of voting machines to, and their use in, election fraud in the 2020 Presidential Election.

e. As a state actor, and acting under color of state law, depriving Plaintiff of his rights of equal protection and due process by bringing sham and potentially ruinous litigation against Plaintiff purely out of discrimination against his political viewpoint, in violation of 42 U.S.C. § 1983.

The facts will further establish that Plaintiff has suffered actual damages as a proximate cause of Defendants' agreement and wrongful overt acts.

VII. DAMAGES AND OTHER RELIEF

157. Plaintiff incorporates the foregoing paragraphs as if fully set forth verbatim below.

158. The facts set out above and to be proven at trial will demonstrate that Plaintiff is entitled to recover against Defendants, jointly and severally, the following:

a. Actual and special damages as allowed by law, in an amount to be proven at trial, including but not limited to the following:

   a. Special damages in the form of attorneys fees and expenses incurred in defending against Dominion's lawsuit;

   b. Damages for defamation *per se* for Dominion's public attacks on his honesty and integrity; and,

   c. Damages to be determined by the trier of fact suffered as a result of the deprivation of his rights under the First Amendment to the U.S.

Constitution and under the "support and advocacy" clause of 42 U.S.C. § 1985(3); together with,

b. Three times actual damages for violations of 18 U.S.C. § 1862;

c. Punitive damages as allowed by law, in an amount to be determined by the trier of fact;

d. Reasonable and necessary attorney's fees, as allowed by law; and,

e. Costs of suit.

VIII. CONDITIONS PRECEDENT

159. All conditions precedent to Plaintiff bringing and maintaining this action have been satisfied or waived.

IX. JURY DEMAND

160. Plaintiff respectfully requests trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff asks that Defendants be cited to answer and appear herein and that, after trial or other hearing on the merits, Plaintiff have and recover against the Defendants, jointly and severally, the relief requested herein, together with all writs and processes necessary to the enforcement of same, and all other relief to which he may show himself justly entitled.

Respectully submitted,

BARNES & THORNBURG LLP

/s/ Alec J. Beck
Minnesota State Bar No. 201133
225 S. Sixth Street, Suite 2800
Minneapolis, Minnesota 55402
(612) 367-8709 (Telephone)
(612) 333-6798 (Facsimile)
alec.beck@btlaw.com

Douglas A. Daniels (*pro hac vice pending*)
Texas State Bar No. 00793579
Heath A. Novosad (*pro hac vice pending*)
Texas State Bar No. 24037199
DANIELS & TREDENNICK, PLLC
6363 Woodway Drive, Suite 700
Houston, Texas 77057
(713) 917-0024 (Telephone)
(713) 917-0026 (Facsimile)
doug.daniels@dtlawyers.com (E-mail)

Attorneys for Plaintiff