IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

THIRD AMENDED COMPLAINT

Plaintiffs Donna Curling, Donna Price, and Jeffrey Schoenberg hereby allege and plead for their Third Amended Complaint as follows:

PRELIMINARY STATEMENT

1. The right to vote is the most fundamental and sacrosanct of all of the rights conferred on U.S. citizens by the Constitution as well as by the Georgia Constitution and Georgia state law. It is the foundation of our democracy. As the Supreme Court has set out in unambiguous terms, "[n]o right is more precious in a free country than that of having a voice in the election of those who make the laws under which, as good citizens, we must live. Other rights, even the most basic, are illusory if the right to vote is undermined." *Wesberry v. Sanders*, 376 U.S. 1, 17 (1964). *See also Wexler v. Anderson*, 452 F.3d 1226, 1232 (III) (11th Cir. 2006)

("The right to vote is fundamental, forming the bedrock of our democracy."). The Georgia Constitution as well reflects the drafters' recognition of the vital role that the right to vote plays in the management of the State's affairs by explicitly providing that "[e]lections by the people shall be by secret ballot and shall be conducted in accordance with procedures provided by law." Ga. Const. Art. II § 1, ¶ 1.

2. In reaction to the profound challenges that emerged from the 2000 Bush-Gore presidential election, many states, Georgia among them, turned to paperless electronic voting systems in the expectation that this technology would prevent a reprise of that election's problems. Plaintiffs raise no questions regarding the intent behind that change. However, over the years, it has been increasingly apparent that paperless electronic voting systems have not, and could not, live up to expectations. Indeed, the system is now known to be so vulnerable to intrusion and manipulation that the nation's leading cybersecurity experts have been going to great lengths to educate both the states and Congress about the perils inherent in those systems, and to urge the return to paper ballots.

3. Despite the inclination to put great faith in the wonders of technology, it is decidedly not the answer when it comes to voting systems. The Direct Recording Equipment ("DRE") voting system ("DRE Voting System") used in

Georgia is a prime illustration of the regrettable incompatibility between the functioning of the current electronic voting system and the voters' right to cast a ballot and have that vote accurately counted. Because of such concerns, states across the country, in increasing numbers, have been returning to the safety of paper ballots, with only five states remaining, like Georgia, using all electronic voting.

4. The inherent vulnerabilities of DREs tremendously compromise the rights of voters in any jurisdiction. Furthermore, the integrity of Georgia's DRE Voting System was significantly eroded as a consequence of the misfeasance and malfeasance of the Defendants: The central server used both to store voters' personal identifying data and to program every electronic voting machine in Georgia was readily accessible in the many months (and possibly years) leading up to the 2016 Presidential election, and subsequent 2017 elections -- and accessible not merely to cybersecurity experts, but to anyone with a modicum of familiarity with computer use. The central server was wide open for anyone to enter the system and readily access personal data of Georgia voters. Furthermore, such an intruder could also easily manipulate the server's data and voter registration software, and thereby render legitimate voters ineligible, add fictitious voters to the

list, and switch votes so as to increase the numbers for the candidate of the intruder's choosing.

5. The gross abrogation of the Constitutional and statutory obligations to protect the franchise rights of Georgia voters did not stop there. Instead, when the security failure was discovered by a local cybersecurity expert and brought to the attention of two of the Defendants, the expert was warned to drop the issue. And it was not only the warnings from this cybersecurity expert that these Defendants ignored. Later, they would turn a blind eye to other critical warnings from more than twenty leading cybersecurity and voting system experts, from the Department of Homeland Security ("DHS"), from the Federal Bureau of Investigation ("FBI"), and from the Election Assistance Commission ("EAC").

6. Indeed, Georgia's Secretary of State ("GA SOS") not only ignored each of these warnings, but also refused the offers of assistance in remedying the problems that the DHS and the FBI urged it to accept. Rather, GA SOS publicized completely unfounded allegations of an attempted takeover of Georgia's electoral system by the federal government.

7. Even under the very best of circumstances – with the current voting systems properly installed, programmed, and operated – the inherent flaws in the DREs render it not possible for the state to comply with the election law or to

protect the rights of Georgia voters. Yet, these are not the best of circumstances; far from it. Rather, there is compelling evidence that the rights of Georgia voters guaranteed by Georgia statute and the U.S. and Georgia constitutions to have their votes counted accurately, have been flagrantly and repeatedly breached by Defendants' conduct.

8. This case is not merely about a technical violation or a theoretical risk. It is about forcing voters to choose between totally relinquishing their right to vote and acquiescing to cast their vote despite very real risks: the risk that their vote will not be properly counted; the risk that the declared results will be contrary to the will of voters; and furthermore, the risk that there will be no way to verify the validity of the election.

9. Any question of convenience of Defendants and their commitment to a woefully flawed and wholly indefensible voting system must not be permitted to take priority over the statutory and Constitutional rights of Georgia voters.

10. This complaint sets forth the violations of law and the other serious irregularities that occurred during the November 8, 2016 General Election, ("2016 General Election"), the April 18, 2017, 6th Congressional District Special Election ("Special Election"), the June 20, 2017, 6th Congressional District Runoff Election ("Runoff"), and the May 2018 and November 2018 General Elections

(collectively, the "Relevant Previous Elections") causing the results of such elections to be indeterminable.

11. This complaint also sets forth violations of law resulting from Defendants' continued failure to implement a constitutionally-acceptable election system. Despite warnings from cybersecurity experts, government officials, and even this Court, Defendants still intend to utilize their flawed DRE Voting System in upcoming elections during Fall 2019. Additionally, while Defendants are implementing a paper ballot system for certain 2020 elections, they have chosen to force all of Georgia's voters to use ballot-marking devices ("BMDs") which suffer from the same security vulnerabilities as Defendants' flawed DRE Voting System.

12. For these reasons and those demonstrated below, Plaintiffs respectfully ask the Court: (1) to hold Defendants liable for the violations of Georgia voters' rights in connection with the Relevant Previous Elections, and to ensure that those rights are protected in connection with the scheduled Fall 2019 and all future elections, (collectively, the "Relevant Pending Elections") and (2) to enter an order providing such relief as is necessary and appropriate to protect Georgia's voters from such future, irreparable harm.

PLAINTIFFS

13. Plaintiffs are electors who are residents of Georgia as well as electors of the State of Georgia who are concerned about the integrity, credibility, security, and reliability of the electoral process. All Plaintiffs have cast ballots in one or more of the Relevant Previous Elections, and all have cast ballots on the DRE Voting System in one or more of the Relevant Previous Elections.

14. DONNA CURLING ("Curling") is an elector of the State of Georgia and a resident of Fulton County. Curling voted in the Relevant Previous Elections, and intends to vote in all future elections for which she is eligible.

15. Due to concerns over the integrity of prior Georgia elections, Curling requested that GA SOS reexamine Georgia's DRE Voting System. Curling also chose to exercise her right to cast her vote using a verifiable paper ballot in the Runoff, so as to ensure that her vote would be permanently recorded on an independent record. To do so, Curling persisted through considerable inconvenience – only to be incorrectly told by GA SOS and the Fulton County Board of Registration and Elections that she had not, in fact, cast a ballot, creating irreparable harm that her ballot was not counted. Without the intervention of this Court, Curling will be compelled to choose between relinquishing her right to vote and acquiescing to cast her vote under a system that violates Georgians' rights and

cannot reliably determine election outcomes that can be legally certified. As such, Curling has standing to bring her claims.

16. Plaintiff DONNA PRICE ("Price") is an elector of the State of Georgia and a resident of DeKalb County. Due to concerns over the integrity of prior Georgia elections, prior to the Runoff, Price joined the group of 13 other electors who exercised their right under O.C.G.A § 21-2-379.2(a) to request that GA SOS reexamine Georgia's DRE Voting System – a request GA SOS effectively denied, abridging her rights to assure that future elections would be conducted on compliant systems. She cast her vote on a DRE in the 2016 General Election, and intends to vote in all future elections for which she is eligible. Without the intervention of this Court, Price will be compelled to choose between relinquishing her right to vote and acquiescing to cast her vote under a system that violates her right to vote and to have her vote accurately counted. As such, Price has standing to bring her claims.

17. Plaintiff JEFFREY SCHOENBERG ("Schoenberg") is an elector of the State of Georgia and a resident of DeKalb County. He cast his ballot on DRE machines in all the Relevant Previous Elections and intends to vote in all future elections for which he is eligible. In casting his ballot in a voting system that abridged his right to participate in a legally conducted election with a determinable

and certifiable result, Schoenberg suffered irreparable harm. Without the intervention of this Court, Schoenberg will be compelled to choose between relinquishing his right to vote and acquiescing to cast his vote under a system that violates his right to vote and to have his vote accurately counted. As such, Schoenberg has standing to bring his claims.

DEFENDANTS

18. Defendant BRAD RAFFENSPERGER ("Secretary Raffensperger") is the Secretary of State of Georgia and, in that role, also serves as Chair of the State Election Board. Secretary Raffensperger's predecessor, current Georgia Governor Brian P. Kemp, was responsible for the Relevant Previous Elections, and Secretary Raffensperger is responsible for the orderly and accurate administration of Georgia's electoral processes and the Relevant Pending Elections. This responsibility includes the duty to ensure that legally compliant voting systems are in place, and to conduct any reexaminations of Georgia's DRE Voting System currently in use, upon request or at his own discretion.

19. Defendants DAVID J. WORLEY, REBECCA N. SULLIVAN, ANH LEE, and SETH HARP ("State Election Board Members") are members of the State Election Board in Georgia. As such, for the Relevant Previous Elections, and, for the Relevant Pending Elections, they were responsible and continue to be

responsible for (1) promulgating rules and regulations to ensure the legality and purity of all elections, (2) investigating fraud and irregularities in elections, and (3) reporting election law violations to the Attorney General or appropriate district attorney.

20. Defendants MARY CAROLE COONEY, VERNETTA NURIDDIN, KATHLEEN D. RUTH, MARK WINGATE, and AARON JOHNSON ("County Election Board Members") are members of the Fulton County Board of Registration and Elections who were, for the Relevant Previous Elections, and, for the Relevant Pending Elections, continue to be, responsible for conducting the elections in Fulton County.

21. All Defendants are sued only in their official capacities.

I. JURISDICTION AND VENUE

22. On August 8, 2017, Defendants consented to jurisdiction when they removed this action on the basis of Federal Question jurisdiction under 28 U.S.C. § 1331. Dkt. No. 1-14.

23. Further, this Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331, 1343, 1367, 2201, and 2202.

24. Venue lies in this court pursuant to 28 U.S.C. § 1391(b) because all reside in the district and a substantial part of the events or omissions giving rise to the Plaintiffs' claims occurred in this judicial district.

II. FACTUAL BACKGROUND

A. Georgia's DRE Voting System is Fundamentally Flawed and Vulnerable

25. Georgia's DRE Voting System relies primarily of the use of DRE voting computers, which, by design, directly record an elector's vote on an electronic medium. *See* O.C.G.A. §§ 21-2-379.1 to -379.12; *see also* Ga. Comp. R. & Regs. 183-1-12.01. The DREs used in Georgia provide no method through which voters can be assured that their vote has been accurately recorded, in contrast with an anonymous paper ballot which the voter marks and reviews before he casts his ballot. DREs produce neither a paper trail nor any other means by which the records of votes cast can be audited.

26. These inherent problems are exacerbated by the fact that Georgia uses DREs that run on antiquated software that is programmed by and downloaded from one central location, the Center for Elections Systems ("CES"), formerly located at Kennesaw State University ("KSU"), and now located within GA SOS's office. Relying on a single site renders Georgia's DRE Voting System far more vulnerable than systems that are managed through numerous sites at the county level across

the state. In Georgia, only one server needs to be compromised in order for an intruder to exploit it, making Georgia elections a tempting target.

27. The Georgia Global Election Management System ("GEMS") is beset by vulnerabilities.

28. Defendants have publicly represented that because Georgia's GEMS database was unique and confidential, hackers could not design malware compatible with that database. In reality, however, the Georgia GEMS database is structured identically to databases that have been available on the internet since 2002. Therefore, by Defendants' own admission, the GEMS system is critically vulnerable.

29. Compounding these concerns is the fact that Georgia has not updated or provided patches to its GEMS database software since approximately 2005.

30. Despite these vulnerabilities, Georgia has not collected all of the approximately 50,000 DRE memory cards employed by Georgia during elections for testing or reformatting since 2013 or 2015. Similarly, Georgia has never tested or otherwise checked the internal memory of its DRE voting machines.

31. In addition to the problems associated with the DRE Voting System in general, and the added vulnerabilities created by Georgia's antiquated software and

single point of entry, Georgia's DRE Voting System has long been at further risk because of gross mismanagement.

32. For example, CES Director Michael Barnes transfers data directly from the GEMS central server using a USB drive to a public computer that is connected to the internet. After being exposed to the internet, this USB drive is then reinserted back into the GEMS server. Notably, while Barnes maintains this USB drive in a locked desk drawer, he leaves the key to this drawer unlocked in the same desk.

33. Additionally, outside contractors working from their own homes on their own personal computers, construct the GEMS database used for Georgia's elections.

B. The Exposure and Breaches of Georgia's DRE Voting System Have Been Undeniably Established

34. In August of 2016, a professional cybersecurity expert residing in Georgia, Logan Lamb ("Lamb"), who was interested in the state's election system, accessed CES's public website. Shockingly, Lamb was able to access key components of Georgia's electronic election infrastructure, without so much as entering a password. It should be noted that these actions were in accordance with both the law and the general standards followed by most professionals in the cybersecurity industry.

35. In accessing these election system files, Lamb found a startling amount of private information, including: driver license numbers, birthdates, and the last four digits of social security numbers for over six-and-a-half million Georgia voters; the passwords given to polling place supervisors on election day to control the opening and closing of the DREs and to make administrative corrections in the event a DRE encountered a problem; and executable programs that could be used to implant malware and vote stealing programs in the system.

36. This publicly available information easily found by Lamb provided everything a bad actor would need to interfere with an election and to manipulate its outcome – while likely avoiding detection.

C. The Defendants' Unwillingness to Recognize and Respond to the Problems

37. Lamb immediately alerted Merle King ("King"), the Georgia official responsible for overseeing, managing, and securing Georgia's electronic election infrastructure, to the serious security vulnerabilities he had discovered. In response, Lamb was cautioned by King that if he talked about it, he would be "crushed by the politicians downtown."

38. Upon information and belief, not only did Georgia fail to take remedial action when alerted to the problem Lamb raised, it failed to act even in the face of the detailed information on the cybersecurity threats facing the nation's

election systems, and the recommended specific steps to reduce the risk, which were disseminated by the FBI, the DHS, and the EAC. The press reported that Georgia was the only state to refuse all federal assistance to help ensure the security of its election infrastructure. Neither did the state officials respond to a letter that had been drafted by a group of over twenty voting system and cybersecurity experts expressing their heightened concerns about Georgia's DRE Voting System.

D. The Consequences of Georgia's Failure to Act

39. In February 2017, a cybersecurity colleague of Lamb's, Chris Grayson ("Grayson"), was able to repeat what Lamb had done seven months earlier. Around that same time, Lamb also found that, not only could he still easily access and download the same information as he had previously done, he discovered additional and updated information, including more recent database files and passwords.

40. Upon information and belief, Grayson notified a colleague and a faculty member at KSU of his findings. This colleague then notified KSU's University Information Technology Services ("UITS") Information Security Office, which in turn notified King. The day after Grayson's notification, the KSU

UITS Information Security Office seized CES's server. Two days after Grayson's notification, the FBI had been alerted and took possession of the server.

41. On at least two occasions prior to the seizure by the FBI, King and CES were made aware of this data breach. KSU issued a press release as to this data breach on March 1, 2017, and press accounts report that GA SOS was aware of this breach by March 3, 2017.

42. In a separate incident, on April 15, 2017, four electronic pollbooks and memory cards containing the PII of voters in Cobb County were stolen. Press accounts have quoted Cobb County election officials as stating that these pollbooks contained state-wide voter information.

43. Upon information and belief, Defendants failed to notify the consumer reporting agencies and the 6.5 million Georgia voters whose personal identifying information had been compromised by the CES system, as required by O.C.G.A § 10-1-912. Their failure to do so exposed those voters to substantially greater risk of their personal data being misused in ways that would harm them. And even after the occurrence of an actual security breach in April 2017 – the theft of electronic pollbooks containing statewide voter registration database and software to program voter access cards – no action was taken to properly report either security breach of voter data.

44. The DRE Voting System did not, and cannot ever, meet Georgia's constitutional statutory requirements, and caused each of the Relevant Previous Elections to generate indeterminable results, abridging numerous state and federal rights of the Plaintiffs and all other Georgia voters.

E. Georgia's Own Experts Have Confirmed These Vulnerabilities

45. GA SOS engaged cybersecurity experts Fortalice to conduct assessments of their cybersecurity infrastructure. Notably, GA SOS did not engage Fortalice to conduct any assessment of its *election* cybersecurity, include its DREs or the GEMS database and servers, despite Fortalice's ability to conduct such analysis.

46. Fortalice identified significant cybersecurity deficiencies with GA SOS's network.

47. For example, in an October 2017 assessment, Fortalice identified twenty-two cybersecurity risks within GA SOS's IT operations, categorizing most of these risks as significant.

48. One of these risks was widespread local administrative rights, meaning that all GA SOS users who had any level of log-in credentials also were granted administrative rights on their work stations. This increased the likelihood that malware or a malicious actor could successfully compromise a user's work

station through email, web, or removal media. GA SOS's experts found that the problem was particularly acute because not only did users have administrative rights on their own work stations, but they also had administrative rights on all work stations. This meant that if an attacker gained access to a single work station, they could quickly access any other work station, gain administrative rights, and spread malware, install remote access tools, or access sensitive data.

49. Another risk identified by Fortalice in their October 2017 assessment was a lack of two-factor authentication for remote access. This meant that GA SOS users were able to remotely access the GA SOS network using only a user name and a password. According to Fortalice, this level of security was insufficient, particularly given the possibility of phishing attacks or the potential theft of GA SOS credentials.

50. Fortalice also expressed an overarching concern for the lack of control and oversight GA SOS was able to maintain over its voter registration database. Indeed, GA SOS employees informed Fortalice that the voter registration database represented GA SOS's greatest cybersecurity vulnerability.

51. As part of its October 2017 assessment, Fortalice conducted a penetration test of GA SOS's networks. Fortalice was able to successfully penetrate GA SOS's network and gain administration rights to that network.

52. In February 2018, Fortalice conducted an additional cybersecurity assessment, focusing on the independent vendor that Georgia retained to manage its voter registration database. Fortalice identified fifteen additional security risks involving Georgia's voter registration database. For example, Fortalice found that the contract between GA SOS and the independent vendor did not contain any cybersecurity requirements. Fortalice found that the vendor was relying on outdated software that was known to contain critical security vulnerabilities. Fortalice noted that an attacker with sufficient time and resources could exploit those vulnerabilities. Fortalice also identified certain remote access vulnerabilities. Specifically, the vendor did not block VPN connections from the IP addresses of known threats or foreign countries. Additionally, Fortalice identified a number of missing critical operating system patches, unsupported software, and vulnerable third-party software.

53. In November 2018, Fortalice conducted a third assessment of GA SOS's cybersecurity. As part of this assessment, Fortalice made an additional twenty recommendations to GA SOS to improve its cybersecurity.

54. Notably, of the twenty-two risks identified by Fortalice in October 2017, only three had been remediated as of November 30, 2018, just weeks after the November 2018 midterm elections.

55. Based on this assessment, on a scale of zero to one hundred, Fortalice graded GA SOS' cybersecurity as a 53.98.

56. Despite the fact that Fortalice had identified significant cybersecurity vulnerabilities with Georgia's voter registration database in its October 2017 and February 2018 assessments, GA SOS instructed Fortalice not to review the voter registration database in November 2018.

57. Notwithstanding Fortalice's warnings, in November 2018, on the eve of an election, it was publicly revealed that Georgia's voter registration database had serious, remotely-exploitable vulnerabilities.

58. Another expert retained by GA SOS, Dr. Michael Shamos, has repeatedly criticized GA SOS's election cybersecurity practices.

59. For example, while Dr. Shamos believes that Georgia should test each memory card before it places it into a DRE machine, upon information and belief, Georgia does not do so.

60. Similarly, while Dr. Shamos believes that Georgia should conduct comparative and forensic analyses to determine whether its DRE machines and software are properly functioning, upon information and belief, Georgia does not do so.

61. Additionally, while Dr. Shamos believes that Georgia should conduct parallel testing on its DRE machines, by selecting at least one machine to test in every single county, upon information and belief, Georgia does not conduct parallel testing in this manner. Instead, Georgia tests only a single machine out of the approximately 27,000 machines used in Georgia elections. Dr. Shamos, Defendants' own expert, does not have confidence in Georgia's testing procedures, which test only one machine out of approximately 27,000.

F. Georgia Failed to Act Despite Growing Threats to U.S. Election Security

62. Georgia's stubborn failure to address these critical security vulnerabilities comes amidst revelations that Russia and other foreign nations are increasingly targeting U.S. election systems with increasing sophistication.

63. The Mueller Report revealed that "[t]he Russian government interfered in the 2016 presidential election in sweeping and systematic fashion." Notably, evidence of Russian interference "began to surface in mid-2016."

64. In July 2018, Special Counsel Robert Mueller released an indictment that confirmed that Georgia was specifically targeted by a Russian operative.

65. The Senate Intelligence Committee confirmed these findings in a bipartisan report. According to the Senate Intelligence Committee, hackers likely tried to access election systems in all fifty states during the 2016 elections. Russia

"directed extensive activity, beginning in at least 2014 and carrying into at least 2017, against U.S. election infrastructure at the state and local level." The report specifically found that "[s]tate election officials, who have primacy in running elections, were not sufficiently warned or prepared to handle an attack from a hostile nation-state actor."

66. The Senate Intelligence Committee noted that Russian operatives engaged in operations to scan the election-related state infrastructure of all fifty states, conducting research on election-related web pages, voter ID information, election system software, and election service companies.

67. Further, Robert Mueller confirmed during his July 2019 testimony to Congress that Russia's interference in our elections continues to this day. And, as he testified, "[m]any more countries are developing the capability to replicate what the Russians have done."

68. Given this extensive risk, cybersecurity experts and government officials have instructed that states implement paper ballot systems with optical scanners that include a voter-verified paper trail.

69. Georgia has ignored this guidance.

G. Georgia's Proposed Election System Remains Unconstitutional

70. In April 2019, Georgia passed H.B. 316, which provided for the use of a paper ballot system to be marked by BMDs. In July 2019, Georgia confirmed that it had awarded the contract for this new system to Dominion Voting Systems, Inc. ("Dominion").

71. The system described in Georgia's contract with Dominion calls for in-precinct scanners/tabulators for 2D barcodes generated by BMDs (the "Proposed Election System"). The BMDs, identified as Image Cast X models, are also capable of producing a text summary, as opposed to an image of the actual ballot, of an elector's candidate selections. The ballot scanners tabulate votes from each ballot based on the 2D barcode generated by the BMD and not based on the written text summary of a voter's selections. Therefore, no elector can visually review and confirm whether the bar code accurately conveys their intended selections.

72. The Proposed Election System will not be substantially safer than the current system because BMDs remain susceptible to manipulation, and the proposed system does not provide a meaningful way for a voter to audit their vote.

73. The 2D barcode produced by the BMD is not readable by a voter, but is relied upon by the precinct scanner to tabulate votes in each precinct. The

legible written summary of a voter's choice is not relied upon by the precinct scanner at all.

74. Therefore, while the Proposed Election System purports to provide a voter with an auditable voting record, the voter is only able to audit the written text summary and not the actual barcode on the ballot used to tabulate votes.

75. In other words, despite the fact that cybersecurity experts and government officials recommended a voting system that included a voter-verified paper trail, the Proposed Election System will rely on a non-voter-verified barcode as the elector's actual vote.

76. Further, these BMD systems have the same demonstrated security vulnerabilities as those that plague Georgia's DREs.

77. Like any computer, a BMD is vulnerable to intentional forms of manipulation (such as hacking, installation of malware, or alteration of installed software), as well as unintentional forms of manipulation (such as bugs and misconfiguration).

78. Indeed, specific vulnerabilities have already been identified with Dominion's election software and hardware.

79. Dominion's election system was certified under a 14-year old standard (Voluntary Voting System Guidelines ("VVSG") 1.0) rather than the more recent VVSG 1.1 or VVSG 2.0 standards.

80. In February 2019, Texas voting systems examiners refused to certify Dominion's election management system based upon several problems with the software. According to these examiners, "several of the problems did not appear to have ready-made or simple solutions." These problems included:

(a) The ability of Dominion's hardware to be connected to the internet;

(b) If the printer tray became ajar during the voting process the system would wipe out all selections and require a voter to start over, therefore requiring poll worker intervention and slowing down the voting process;

(c) The audit trail stored voter selections in sequential order, which would permit the secrecy of the ballot box to be compromised;

(d) Portions of the power cord connections are easily accessible and may be unplugged by anyone;

(e) The paths for import of election data into the election management program revealed multiple opportunities for mistakes

and during testing required three separate restarts of the adjudication process.

81. During the 2019 DEFCON Voting Village,[1] Dominion's precinct scanners were made available to participating hackers. These hackers identified twenty vulnerabilities. One vulnerability was the ability of remote attackers to implement a DNS attack. Another vulnerability was the existence of an exposed flash card containing an .xml file that, if manipulated, would allow for scanned votes to be redirected to a different candidate.

82. Additionally, the ImageCast X BMDs rely on software released in February 2015, which has not received security updates since March 2018.

83. These many vulnerabilities could cause the BMD to print votes to the 2D barcode that do not match what the voter entered, or could cause a precinct scanner to improperly tabulate votes.

84. Moreover, these vulnerabilities are not alleviated by the text summary available to an elector, because the 2D barcode actually relied upon to tabulate the vote may not necessarily match the text summary.

[1] DEFCON is a hacking conference held annually since its founding in 1993. Since 2017, DEFCON has featured a Voting Machine Hacking Village, in which hackers attempt to infiltrate U.S. election infrastructure such as voting machines, registration databases, and election office networks, to highlight potential cybersecurity vulnerabilities.

85. Further, even if the 2D barcode is identical to the text summary, research has demonstrated that most voters are unlikely to review these summaries even when specifically directed to do so.

86. Additionally, polling place exit interviews of voters who do choose to review a text summary of their vote reveal that some are unable to recall details of the ballots they cast even moments before. Voters fail to recognize errors in ballots presented to them for verification, or fail to recognize that the ballots presented to them for verification were not the ones they actually cast.

87. On those occasions where a voter does notice a discrepancy in a 2D barcode, research suggests that they are far more likely to attribute the discrepancy to their own mistake. Therefore, they are unlikely to raise concerns about a systemic attack on an election.

88. Even Dr. Shamos, the expert retained by GA SOS with respect to its election cybersecurity testified that if a BMD is going to be used, the more reliable approach is to use a BMD that produces a ballot readable by a human voter, rather than a bar code.

89. Georgia's Proposed Election System is also susceptible to manipulation because Georgia has not committed to risk-limiting audits for its

upcoming elections.[2] The limited assurance offered by the Proposed Election System's barcode verification is undermined by the absence of any commitment to actually auditing those barcodes.

90. For these reasons, Georgia's Proposed Election System provides Georgia's voters with no greater guarantee than the current system that their votes will be accurately recorded and tabulated.

III. CLAIMS

COUNT I: VIOLATION OF FUNDAMENTAL RIGHT TO VOTE UNDER THE DUE PROCESS CLAUSE OF THE 14TH AMENDMENT AND OF 42 U.S.C. § 1983

(All Plaintiffs against All Defendants in their Official Capacities)

91. Plaintiffs incorporate the allegations of paragraphs 1 through 90 above as if expressly realleged herein.

92. The right to vote is a fundamental right protected by the Due Process Clause of the Fourteenth Amendment of the U.S. Constitution.

93. The fundamental right to vote encompasses the right to have that vote counted accurately, and it is protected by the Due Process Clause of the Fourteenth Amendment of the U.S. Constitution.

[2] For example, the National Academies of Sciences, Engineering, and Medicine's September 2018 report regarding voting system integrity recommended the use of risk-limiting audits, in which individual randomly selected paper ballots are examined until sufficient statistical assurance as to the integrity of an election is achieved.

94. Defendants violated Plaintiffs' fundamental right to vote by deploying a DRE voting equipment system that by its design and management by Defendants:

(a) Failed to provide reasonable and adequate protection against the real and substantial threat of electronic and other intrusion and manipulation by individuals and entities without authorization to do so;

(b) Failed to include the minimal and legally required steps to ensure that such equipment could not be operated without authorization; to provide the minimal and legally required protection for such equipment to secure against unauthorized tampering; to test, inspect, and seal, as required by law, the equipment to ensure that each DRE unit would count all votes cast and that no votes that were not properly cast would not be counted; and to ensure that all such equipment, firmware, and software is reliable, accurate, and capable of secure operation as required by law;

(c) Failed to provide a reasonable and adequate method for voting by which Georgia electors' votes would be accurately counted.

95. By choosing to move forward in using the non-compliant system, Defendants willfully and negligently abrogated their statutory duties and abused their discretion, subjecting voters to cast votes on an illegal and unreliable system—a system that must be presumed to be compromised and incapable of producing verifiable results.

96. Upon information and belief, despite their knowledge that the DRE Voting System does not comply and cannot be made to comply with the Election Code, these Defendants willfully and knowingly plan to continue to use this non-compliant system in the Relevant Pending Elections.

97. Upon information and belief, Plaintiffs received no notice that their votes under the DRE Voting System could not be counted accurately due to Defendants' material non-compliance with the Election Code.

98. Defendants' violation of the Due Process Clause is patently and fundamentally unfair and therefore relief under 42 U.S.C. § 1983 is warranted. Accordingly, Plaintiffs ask this Court to (a) declare that these Defendants violated the Due Process Clause of the Fourteenth Amendment; (b) enjoin Defendants' use of Georgia's DRE Voting System for future elections; and (c) award attorneys' fees and costs for Defendants' causation of concrete injury to Plaintiffs, whose fundamental right to have their vote counted as cast was thwarted.

COUNT II: VIOLATION OF FUNDAMENTAL RIGHT TO VOTE UNDER THE EQUAL PROTECTION CLAUSE OF THE 14TH AMENDMENT AND OF 42 U.S.C. § 1983

(All Plaintiffs against All Defendants in their Official Capacities)

99. Plaintiffs incorporate the allegations of paragraphs 1 through 90 above as if expressly realleged herein.

100. The Equal Protection Clause of the Fourteenth Amendment mandates that "[n]o State shall . . . deny to any person within its jurisdiction the equal protection of the laws." U.S. Const. amend. XIV § 1.

101. The Equal Protection Clause protects the manner of the exercise of the right to vote, and a state may not value one person's vote over that of another. U.S. Const. amend. XIV § 1.

102. Upon information and belief, GA SOS and the County Election Board Members allowed electors to vote in the Relevant Previous Elections using two different methods: (a) voting using the DRE Voting System and (b) voting using paper ballots (available to provisional and absentee voters).

103. Upon information and belief, absentee paper ballots are verifiable, recountable ballots, which can be counted, reviewed, and discrepancies corrected under the supervision of a court.

104. DRE ballots are counted electronically and cannot reliably prevent or detect errors or reliably determine the election results. The DRE Voting System:

(a) Produces only an electronic representation of a vote, with no independent reference document, and cannot therefore provide for a means by which the accuracy of the recording of DRE ballots can be tested or verified;

(b) Does not provide reasonable and adequate protection, as required by the Georgia Election Code, against the real and substantial threat of electronic and other intrusion and manipulation by individuals and entities without authorization to do so; or

(c) Provide a reasonable and adequate method for voting by which Georgia electors' votes would be accurately counted.

105. The injuries suffered by Georgia electors were compounded dramatically by Defendants' failure to include the minimal and legally required steps to ensure that such equipment could not be manipulated or operated without authorization; to provide the minimal and legally required protection for such equipment to secure against unauthorized tampering; to test, inspect, and seal as required by law the equipment to ensure that the DRE Voting System would properly count all cast votes and discount any improperly cast votes; and to ensure

that all such equipment, firmware, and software is reliable, accurate, and capable of secure operation as required by law, and properly certified to comply with Georgia Election Code and Election Rules.

106. Upon information and belief, these Defendants failed to take such steps to attempt to mitigate the security failures, and conduct an election on a system that could comply with the Georgia Election Code. Instead, they continued to rely on the DRE Voting System knowing that this voting system was unsecured, breached, and compromised, could not be presumed to be safe, and was materially non-compliant with applicable Election Code statutes and governing regulations.

107. By choosing to move forward in using the non-compliant system, Defendants willfully and negligently abrogated their statutory duties and abused their discretion, subjecting voters to cast votes on an illegal and unreliable system—a system that must be presumed to be compromised and incapable of producing verifiable results.

108. The voters of the respective ballots have not been treated equally in that the votes of those who voted by DRE cannot be meaningfully recounted, reviewed against an independent record to verify, or have discrepancies detected and corrected. DRE votes are unequally weighted, with greater weight given to those who vote by absentee paper ballot, whose votes can be verified as to voter

intent, can be accurately recounted, and can have processing errors identified and corrected, while votes cast by DRE, whose votes do not share those essential advantages.

109. The rights of Georgia electors using DRE voting equipment to cast their ballots in the Relevant Previous Elections were also not treated equally by virtue of the egregious security failures in the CES election management server. Although the CES security failures put all voting system components at risk, the majority of the security failures could be mitigated for paper ballot votes, but not for DRE votes. In an election contest, the paper ballots could be counted manually and voter intent and accurate tabulation determined, regardless of security failures that may impact DRE Voting System tabulations. DRE Voting System failures cannot be so mitigated nor the impact determined, creating unequal weighting between the two types of ballots cast.

110. The Plaintiffs who voted in Relevant Previous Elections using the DRE Voting System are all similarly situated to other registered electors in the same elections who voted using the DRE Voting System. All Plaintiffs are eligible to vote in the Relevant Pending Elections which may employ the improper DRE Voting System.

111. Defendants' conduct described herein violated the Fourteenth Amendment right of these Plaintiffs to enjoy equal protection of the law.

112. Accordingly, Plaintiffs ask this Court to (a) declare that these Defendants violated the Equal Protection Clause of the Fourteenth Amendment; (b) enjoin Defendants' use of Georgia's DRE Voting System for future elections; and (c) award attorneys' fees and costs for Defendants' causation of concrete injury to Plaintiffs, whose fundamental right to have their vote counted as cast was unequally burdened.

COUNT III: VIOLATION OF FUNDAMENTAL RIGHT TO VOTE UNDER THE DUE PROCESS CLAUSE OF THE 14TH AMENDMENT AND OF 42 U.S.C. § 1983

(All Plaintiffs against All Defendants in their Official Capacities)

113. Plaintiffs incorporate the allegations of paragraphs 1 through 90 above as if expressly realleged herein.

114. The right to vote is a fundamental right protected by the Due Process Clause of the Fourteenth Amendment of the U.S. Constitution.

115. The fundamental right to vote encompasses the right to have that vote counted accurately, and it is protected by the Due Process Clause of the Fourteenth Amendment of the U.S. Constitution.

116. Defendants threaten to violate Plaintiffs' fundamental right to vote by deploying the Proposed Election System that by its design:

(a) Fails to provide reasonable and adequate protection against the real and substantial threat of electronic and other intrusion and manipulation by individuals and entities without authorization to do so;

(b) Fails to include the minimal and legally required steps to ensure that such equipment cannot be operated without authorization; to provide the minimal and legally required protection for such equipment to secure against unauthorized tampering; to test, inspect, and seal, as required by law, the equipment to ensure that all properly cast votes are counted and that votes improperly cast are not counted; and to ensure that all such equipment, firmware, and software is reliable, accurate, and capable of secure operation as required by law;

(c) Fails to provide a reasonable and adequate method for voting by which Georgia electors' votes will be accurately counted.

117. By choosing to move forward with the Proposed Election System, Defendants willfully and negligently abrogated their statutory duties and abused their discretion, subjecting voters to cast votes on an illegal and unreliable

system—a system that must be presumed to be compromised and incapable of producing verifiable results.

118. Upon information and belief, despite their knowledge that the Proposed Election System does not comply and cannot be made to comply with the Election Code, these Defendants willfully and knowingly plan to use this system in the Relevant Pending Elections.

119. Defendants' violation of the Due Process Clause is patently and fundamentally unfair and therefore relief under 42 U.S.C. § 1983 is warranted. Accordingly, Plaintiffs ask this Court to (a) declare that Defendants' Proposed Election System violates the Due Process Clause of the Fourteenth Amendment; (b) enjoin Defendants' use of the Proposed Election System for future elections; and (c) award attorneys' fees and costs for Defendants' causation of concrete injury to Plaintiffs, whose fundamental right to have their vote counted as cast will be thwarted.

COUNT IV: VIOLATION OF FUNDAMENTAL RIGHT TO VOTE UNDER THE EQUAL PROTECTION CLAUSE OF THE 14TH AMENDMENT AND OF 42 U.S.C. § 1983

(All Plaintiffs against All Defendants in their Official Capacities)

120. Plaintiffs incorporate the allegations of paragraphs 1 through 90 above as if expressly realleged herein.

121. The Equal Protection Clause of the Fourteenth Amendment mandates that "[n]o State shall . . . deny to any person within its jurisdiction the equal protection of the laws." U.S. Const. amend. XIV § 1.

122. The Equal Protection Clause protects the manner of the exercise of the right to vote, and a state may not value one person's vote over that of another. U.S. Const. amend. XIV § 1.

123. Upon information and belief, GA SOS and the County Election Board Board Members plan on allowing electors to vote in the Relevant Pending Elections using two different methods: (a) voting using the Proposed Election System and (b) voting using paper ballots (available to provisional and absentee voters).

124. Upon information and belief, absentee paper ballots are verifiable, recountable ballots, which can be counted, reviewed, and discrepancies corrected under the supervision of a court.

125. The Proposed Election System, particularly its BMD system which generates an unreadable 2D barcode, cannot reliably prevent or detect errors or reliably determine the election results. The Proposed Election System:

(a) Produces an unreadable 2D barcode to generate vote totals, and cannot therefore provide for a means by which its accuracy can be tested or verified;

(b) Does not provide reasonable and adequate protection, as required by the Georgia Election Code, against the real and substantial threat of electronic and other intrusion and manipulation by individuals and entities without authorization to do so; and

(c) Does not provide a reasonable and adequate method for voting by which Georgia electors' votes would be accurately counted.

126. The injuries likely to be suffered by Georgia electors will be compounded dramatically by Defendants' failure to include the minimal and legally required steps to ensure that such equipment cannot be manipulated or operated without authorization; to provide the minimal and legally required protection for such equipment to secure against unauthorized tampering; to test, inspect, and seal, as required by law, the equipment to ensure that the Proposed Election System will count all votes cast and that no votes that were not properly cast for that election would be counted; and to ensure that all such equipment, firmware, and software is reliable, accurate, and capable of secure operation as

required by law, and properly certified to comply with Georgia Election Code and Election Rules.

127. Upon information and belief, these Defendants failed to take such steps to attempt to mitigate the security failures, and conduct an election on a system that could comply with the Georgia Election Code. Instead, they intend to rely on the Proposed Election System knowing that this system is unsecured, could be breached and compromised, cannot be presumed to be safe, and is materially non-compliant with applicable Election Code statutes and governing regulations.

128. By choosing to move forward in using the proposed non-compliant system, Defendants willfully and negligently abrogated their statutory duties and abused their discretion, subjecting voters to cast votes on an illegal and unreliable system—a system that must be presumed to be compromised and incapable of producing verifiable results.

129. The voters of the respective ballots have not been treated equally in that the votes of those who will vote using the Proposed Election System cannot be meaningfully recounted, reviewed against an independent record to verify, or have discrepancies detected and corrected. These votes are unequally weighted, with greater weight given to those who vote by absentee paper ballot, whose votes can be verified as to voter intent, can be accurately recounted, and can have processing

errors identified and corrected, while votes cast under the Proposed Election System, whose votes do not share those essential advantages.

130. The Plaintiffs who intend to vote in the Relevant Pending Elections using the Proposed Election System are all similarly situated to other registered electors in the same elections who will vote using the Proposed Election System. All Plaintiffs are eligible to vote in the Relevant Pending Elections which may utilize the Proposed Election System.

131. Defendants' conduct described herein violates the Fourteenth Amendment right of these Plaintiffs to enjoy equal protection of the law.

132. Accordingly, Plaintiffs ask this Court to (a) declare that the Proposed Election System violates the Equal Protection Clause of the Fourteenth Amendment; (b) enjoin Defendants' use of the Proposed Election System for future elections; and (c) award attorneys' fees and costs for Defendants' causation of concrete injury to Plaintiffs, whose fundamental right to have their vote counted as cast will be unequally burdened.

COUNT V: DECLARATORY JUDGMENT

Declaring that the Proposed Election System Violates Act No. 24, H.B. 316

(All Plaintiffs Against All Defendants In Their Official Capacities)

133. Plaintiffs incorporate the allegations of paragraphs 1 through 90 above as if expressly realleged herein.

134. Act No. 24, House Bill No. 316 provides that "[a]s soon as possible . . . all federal, state, and county general primaries and general elections as well as special primaries and special elections in the State of Georgia shall be conducted with the use of scanning ballots marked by electronic ballot markers." The law further provides "that such electronic ballot markers shall produce paper ballots which are marked with the elector's choices in a format readable by the elector."

135. "Scanning ballot" is defined, in relevant part, as "a printed paper ballot designed to be marked by an elector with a ballot marking device or electronic marker or a blank sheet of paper designed to be used in a ballot marking device or electronic ballot marker, which is then inserted for casting into a ballot scanner."

136. "Electronic ballot marker" is defined, in relevant part, as "an electronic device that . . . uses electronic technology to independently and privately mark a paper ballot at the direction of an elector . . . and print an elector verifiable paper ballot."

137. The Proposed Election System violates the clear mandates of Act No. 24, H.B. 316.

138. Instead of producing "paper ballots which are marked with the elector's choices in a format readable by the elector," the Proposed Election System's BMDs produce an illegible and unverifiable 2D barcode along with a text summary of an elector's choices.

139. Similarly, the proposed BMDs do not print an "elector verifiable paper ballot." Instead, the proposed BMDs produce a 2D barcode purportedly constituting an elector's paper ballot that is unverifiable by that elector.

140. Accordingly, Plaintiffs request that the Court declare that the Proposed Election System violates Act No. 24, H.B. 316.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully ask this court:

141. To grant declaratory relief deeming that Defendants have violated the Georgia Constitution, the Fourteenth Amendment to the U.S. Constitution, 42 U.S.C. § 1983, and Georgia election law, including Georgia's system certification regulations and safety and security provisions;

142. To grant injunctive relief prohibiting Defendants from using any system or devices for voting, including, but not limited to, the DRE Voting System and the Proposed Election System, that does not fully satisfy the obligations of the Defendants under Georgia Code Sections 21-2-322, 21-2-379.1(8), 21-2-379.2 (a),

21-2-379.2 (b), 21-2-379.2 (c), 21-2-379.6 (a), 21-2-379.6 (c), 21-2-379.7 (b), 21-2-379.7 (c), 21-2-379.7 (d)(3), 21-2-379.9 (b), 21-2-379.22(6), 21-2-379.22(8), 21-2-379.23(d), 21-2-379.24, and 21-2-379.26; Georgia Rule and Regulation Section 590-8-1-.01(a)(3); and Georgia Constitution Article II, Section 1, Paragraph 1 that protect the rights of Georgia electors under Georgia law and under the Fourteenth Amendment to the U.S. Constitution and 42 U.S.C. § 1983.

143. To grant an Order directing Defendants to submit to the Court within thirty days of entry of the Court's Order a plan providing in sufficient detail for the Court to evaluate the specific steps they intend to take to comply with the terms of the Court's Order.

144. To award attorneys' fees and costs for the deprivation of civil rights arising from alleged Defendants' patent and fundamental unfairness in conducting elections on Georgia's Voting System, causing 42 U.S.C. § 1983 violations; and

145. To grant all other relief this Court deems proper.

Dated: August 16, 2019

Respectfully submitted,

/s/ David D. Cross

David D. Cross
(admitted *pro hac vice*)
John P. Carlin
(admitted *pro hac vice*)
Robert W. Manoso
(admitted *pro hac vice*)
Jane P. Bentrott
(admitted *pro hac vice*)
MORRISON & FOERSTER LLP
2000 Pennsylvania Avenue, NW
Suite 6000
Washington, DC 20006
Telephone: (202) 887-1500
DCross@mofo.com
JCarlin@mofo.com
JBentrott@mofo.com
RManoso@mofo.com

Halsey G. Knapp, Jr.
GA Bar No. 425320
Adam M. Sparks
GA Bar No. 341578
KREVOLIN & HORST, LLC
1201 West Peachtree Street, NW
Suite 3250
Atlanta, GA 30309
Telephone: (404) 888-9700
HKnapp@khlawfirm.com
Sparks@khlawfirm.com

Counsel for Plaintiffs Donna Curling, Donna Price & Jeffrey Schoenberg

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRIAN RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing document has been prepared in accordance with the font type and margin requirements of LR 5.1, using font type of Times New Roman and a point size of 14.

/s/ David D. Cross
David D. Cross

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRIAN RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CERTIFICATE OF SERVICE

I hereby certify that on August 16, 2019, a copy of the foregoing was electronically filed with the Clerk of Court using the CM/ECF system, which will automatically send notification of such filing to all attorneys of record.

/s/ David D. Cross
David D. Cross