IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
(Alexandria Division)

MARK BRADLEY, individually and on behalf of all persons similarly situated, Plaintiff, v. DOMINION DENTAL SERVICES USA, INC., DOMINION DENTAL SERVICES, INC., CAPITAL ADVANTAGE INSURANCE COMPANY, CAPITAL BLUECROSS, and PROVIDENCE HEALTH PLAN, Defendants.	CIVIL ACTION NO: **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Mark Bradley, individually and on behalf of all persons similarly situated, brings this Class Action Complaint against Defendants Dominion Dental Services USA, Inc., Dominion Dental Services, Inc., Capital Advantage Insurance Company, Capital BlueCross (together "Dominion National") and Providence Health Plan (collectively "Defendants") based upon his personal knowledge as to his own experience and on information and belief as to other matters:

INTRODUCTION

1. Dominion National provides insurance and administrates dental and vision benefits offered by other insurers. Customers of Dominion National and the insurers for whom Dominion National provides benefits administration must provide sensitive personal, financial, and medical information to obtain services, which Dominion National retains in its databases.

Customers believe—and expect—that Dominion National will take all necessary precautions to keep their information safe from unauthorized third parties and malicious actors.

2. In fact, Dominion National is legally and contractually obligated to and promised its customers that it would implement and maintain reasonable and adequate safeguards and comply with industry standards in data security practices.

3. Dominion National breached its obligations to and contracts with the consumers it served. On June 21, 2019, Dominion National announced that it had suffered a massive data breach: for nearly nine years, hackers accessed the confidential personal information of nearly three million individuals.

4. From August 2010 until April 2019, hackers exploited vulnerabilities in Dominion National's security systems specifically to access databases containing not only the sensitive and confidential personal, financial and medical information of its own current and former plan members, but also the members of plans like Providence Health Plan, for which Dominion National provides administrative services for dental and vision benefits.

5. According to Dominion National, it discovered the breach after receiving an "internal alert" which prompted it to seek the assistance of the cyber-security firm FireEye Mandiant to conduct an investigation. On June 21, 2019, Dominion National released a statement claiming:

> On April 24, 2019, through our investigation of an internal alert, with the assistance of a leading cyber security firm, we determined that an unauthorized party may have accessed some of our computer servers. The unauthorized access may have occurred as early as August 25, 2010. After learning of this, we moved quickly to clean the affected servers and implement enhanced monitoring and alerting software. We also contacted the FBI and will continue to work with them during their investigation.[1]

[1] https://www.dominionnationalfacts.com/

6. Dominion National's accessed databases contained names, addresses, email addresses, dates of birth, social security numbers, taxpayer identification numbers, bank account and routing numbers, plan identification information such as group numbers, subscriber numbers, and member ID numbers ("personally identifiable information" or "PII")[2] and other protected health information ("PHI") as defined and protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

7. Among other things, Dominion National failed to: 1) adequately secure its databases containing PII and PHI; 2) detect attacks on its system; 3) detect the presence of hackers inside its systems; 4) implement industry-standard security protocols and practices; and 5) investigate whether its security systems were secure.

8. Dominion National's failure to adequately secure and safeguard the PII and PHI in its care violated its express and implied contractual agreements with its customers and its obligations under HIPAA. These failures led to the data breach at issue and the exposure of nearly 3 million individuals' personal information to malicious actors who specifically targeted and obtained Plaintiff and Class Members' personal information located on Dominion National's servers. Plaintiff and the Class Members he seeks to represent did not, therefore, receive the benefits of their bargains with Dominion National or the insurance companies who contracted with Dominion National for plan administration services. Dominion National has also indefinitely exposed Plaintiff and Class Members to or significantly increased the imminent risk of identity theft, financial fraud, medical fraud, or other similar fraudulent activity.

[2] https://www.dominionnationalfacts.com/

PARTIES

9. Plaintiff Mark Bradley is a resident and citizen of Portland, Oregon.

10. Defendant Dominion Dental Services USA, Inc. is a licensed administrator of dental and vision benefits with its principal place of business in Arlington, Virginia. It is a wholly-owned subsidiary of Defendant Capital Advantage Insurance Company.

11. Defendant Dominion Dental Services, Inc. is an insurance company with its principal place of business in Arlington, Virginia. It is a wholly-owned subsidiary of Defendant Capital Advantage Insurance Company.

12. Defendant Capital Advantage Insurance Company is an insurance company with its principal place of business in Harrisburg, Pennsylvania. It is a wholly-owned subsidiary of Capital BlueCross.

13. Defendant Capital BlueCross is a health insurance company with its principal place of business in Harrisburg, Pennsylvania.

14. Defendant Providence Health Plan is an Oregon insurance company with its principal place of business in Beaverton, Oregon.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d). The amount in controversy exceeds $5 million, there are more than 100 putative class members, some of whom are from a different state than Defendants.

16. This Court may exercise personal jurisdiction over Dominion National Dental Services USA, Inc. and Dominion Dental Services, Inc. because both are headquartered in and maintain their principal places of business in Arlington, Virginia which is within this District

and Division. Dominion National also makes decisions regarding data security, issues its notices regarding data security, and implements its decisions regarding data security in this District.

17. The Court may exercise personal jurisdiction over Capital Advantage and Capital BlueCross because they both regularly conduct business in Virginia and have sufficient minimum contacts with Virginia. It was therefore reasonably foreseeable that they could be hauled into Court in Virginia for claims arising out of its provision of health insurance services, including contracting and coordinating with Dominion National Dental Services and Dominion Dental Services in Virginia. The exercise of personal jurisdiction over Capital Advantage and Capital BlueCross in Virginia does not offend traditional notions of fair play and substantial justice.

18. This Court may exercise personal jurisdiction over Providence Health Plan because it contracts with Dominion National, which is located in this District and Division, to provide dental plan administration. It provides its subscriber's personal information to Dominion National in this District and Division. Accordingly, it was reasonably foreseeable to Providence Health Plan that it could be hauled into Court in Virginia for claims arising out of this contract and the disclosure of confidential information thereunder. The exercise of personal jurisdiction over Providence Health Plan would not offend traditional notions of fair play and substantial justice.

19. Venue is proper in this District under 28 U.S.C. § 1391 because Dominion National is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. Dominion National provides dental insurance and administers dental and vision plans.

20. Dominion National is a dental insurer and dental and vision plan benefits administrator. It primarily operates in the mid-Atlantic, but also provides services in Oregon. Dominion describes itself as a "groundbreaker, bringing practical solutions, best practices and a new level of service to the benefits industry. Details are important to us. We guarantee everything from reporting and billing accuracy to network retention and member satisfaction. No point is too fine."[3]

21. All of the Dominion National defendants and other entities are wholly-owned subsidiaries of Capital Advantage Insurance Company, which is itself a wholly-owned subsidiary of Capital BlueCross.

22. Defendant Providence Health Plan is an insurance provider based in and providing health insurance services in Oregon. It contracts with Dominion National to administer its dental plan benefits.

B. Dominion National collects Sensitive Information that is valuable on the black market and is a long-known target of malicious cyber actors.

23. As part of both providing insurance coverage and administering plan benefits under other providers' insurance plans, Dominion National collects a substantial amount of sensitive personal, financial, and medical information from consumers—PII and PHI. This information includes a combination of names, addresses, email addresses, dates of birth, social security numbers, taxpayer identification numbers, bank account and routing numbers, plan identification information such as group numbers, subscriber numbers, and member ID numbers, and other protected health information as defined by HIPAA.

[3] https://dominionnational.com/about

24. PII and PHI are highly valuable on the black market and companies that store large amounts of this information are prime targets of cyber criminals who seek to obtain this information. PII and PHI are valuable on the black market—or the electronic dark web—because it can be used not only to commit identity theft (like opening new credit accounts or filing false tax returns), but also to commit medical identity theft and fraud like stealing prescription drugs or creating false medical IDs. Medical data is particularly valuable because unlike financial information—like credit card numbers—which can often be quickly changed, medical data is static.

25. Because they maintain large databases of this valuable information, medical insurance companies have long been targets of hackers and other malicious actors. For example, in 2012 and 2013, Verizon Business, a leading data breach industry consultant, reported on the prevalence of hacking and malware threats, with breaches in the Health Care and Social Assistance industries making up over 7% of total breaches worldwide.

26. The federal government has also issued warnings that the health insurance sector was particularly prone to cyber-attacks. On April 8, 2014, for example, the Federal Bureau of Investigation's Cyber Division issued a Private Industry Notification to companies within the healthcare sector, stating that the health care industry was a particularly susceptible target for cyber-attacks. The Notification warned that: "[t]he health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely."[4] In August 2014, the FBI again warned that it has observed malicious actors targeting healthcare related systems, perhaps for the purpose of

[4] FBI CYBER DIVISION, PRIVATE INDUSTRY NOTIFICATION: HEALTH CARE SYSTEMS AND MEDICAL DEVICES AT RISK FOR INCREASED CYBER INTRUSIONS FOR FINANCIAL GAIN (Apr. 8, 2014) (available at https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf)

obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[5]

27. And this was not merely a hypothetical threat. Many health insurance providers have announced that they have been targeted by cyber criminals and had data exposed since the FBI's April 2014 warning—and many had allowed the hackers to remain in their systems for years.

28. In 2014, hackers infiltrated Community Health Systems, Inc.'s systems and exfiltrated 4.5 million patients' data.[6]

29. In February 2015, Anthem, Inc. disclosed that it had suffered a massive data breach compromising the personal information of 80 million patient records, including "social security numbers, birthdays, addresses, email and employment information and income data for customers and employees."[7]

30. In March 2015, Washington-based Premera Blue Cross announced that it too had suffered a massive data breach that exposed the personal, financial, and medical data of 11 million customers[8], including "names, dates of birth, addresses, telephone numbers, email addresses, Social Security numbers, member identification number, medical claims information

---

[5] FBI CYBER DIVISION, FBI LIAISON ALERT SYSTEM #A-000039-TT (available at https://info.publicintelligence.net/FBI-TargetingHealthcare.pdf)

[6] Jose Pagliery, *Hospital Network hacked, 4.5 million records stolen*, CNN BUSINESS (Aug. 18, 2014), https://money.cnn.com/2014/08/18/technology/security/hospital-chs-hack/index.html

[7] Reed Abelson & Matthew Goldstein, *Anthem Hacking Points to Security Vulnerability in Health Care Industry*, N.Y. TIMES, (Feb. 5, 2015), https://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html

[8] Kate Vinton, *Premera Blue Cross Breach May Have Exposed 11 Million Customers' Medical And Financial Data*, FORBES, (Mar. 17, 2015), https://www.forbes.com/sites/katevinton/2015/03/17/11-million-customers-medical-and-financial-data-may-have-been-exposed-in-premera-blue-cross-breach/#59caea2a75d9

and financial information."[9]

31. In September 2015, Excellus BlueCross BlueShield in New York announced that as many as 10 million of its customers' personal data was exposed in a data breach that dated back to 2013, including "names, dates of birth, Social Security numbers, mailing addresses, telephone numbers, member identification numbers, financial account information and claim information."[10]

32. In 2015, Consumer Affairs reported that 81% of major healthcare or insurance companies had a data breach in the previous two years.[11]

33. And healthcare data breaches are on the rise. In its 2019 Data Breach Investigations Report, Verizon reported that 15% of breaches in 2018 involved Healthcare organizations.[12] Verizon found that 83% of healthcare breaches were motivated by financial gain.[13] Insurance companies are particularly targeted. Verizon reported 927 incidents with 207 confirmed data disclosures in the financial and insurance sectors in 2018, with financial gain making up 88% of the motivation of malicious actors targeting the industry.[14]

34. HIPAA Journal recently reported that "there has been a general upward trend in the number of records exposed each year, with a massive increase in 2015" and that "the main

---

[9] CYBERATTACK INFORMATION FOR PREMERA MEMBERS, https://www.premera.com/wa/visitor/healthsource/community/cyberattack-info/

[10] https://www.usatoday.com/story/tech/2015/09/10/cyber-breach-hackers-excellus-blue-cross-blue-shield/72018150/

[11] *Cyber breach hits 10 million Excellus healthcare customers*, (Sept. 10, 2015), https://www.consumeraffairs.com/news/at-least-81-of-major-healthcare-or-health-insurance-companies-had-a-data-breach-in-the-past-two-years-090415.html

[12] VERIZON BUSINESS READY, 2019 DATA BREACH INVESTIGATIONS REPORT (2019), (available at https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf)

[13] *Id.* at 44.

[14] *Id.* at 41.

causes of healthcare data breaches is now hacking/IT incidents, with unauthorized access/disclosures also commonplace."[15]

C. Dominion National promised that it would protect consumer data.

35. Dominion National was aware of the substantial—and increasing—risk of cyber attackers infiltrating its security systems to access the trove of customer data maintained in its databases.

36. Indeed, Dominion National issued several policies covering the use of sensitive customer data.

37. Dominion National's 2019 Code of Conduct—which sets forth Dominion National's expressed "commitment" to "conducting business with integrity"—specifically acknowledges and addresses the fact that its customers entrust Dominion National with their PII and PHI. It states "we are ***committed*** to protecting confidential information, including employee and member information. . . . Dominion is ***committed*** to protecting the Protected Health Information (PHI) of its members."[16] According to Dominion National, "demonstrating integrity in the workplace means . . . being aware of . . . [p]rotecting Dominion confidential and proprietary information, [and] [s]afeguarding Members' PHI."[17]

38. Dominion National's Code of Conduct further acknowledges that it "sends, receives, uses, and maintains large volumes of Member information. Our Members trust us with some of their most sensitive information. It is our obligation to diligently protect the

[15] HEALTHCARE DATA BREACH STATISTICS, https://www.hipaajournal.com/healthcare-data-breach-statistics/

[16] DOMINION NATIONAL, 2019 CODE OF CONDUCT (2019) (available at https://dominionnational.com/sites/default/files/Misc/2019%20Dominion%20Code%20of%20Conduct.pdf) (emphasis added).

[17] *Id.*

privacy and the security of that information. Most Member information is considered PHI, whether used alone or in connection with other medical or dental information such as diagnosis, procedure codes, and medical or dental records, and includes, but is not limited to:

- Name.
- Address.
- Social security number.
- Date of birth.
- Date of service.
- Contract number.

As employees of Dominion, we are each responsible for ensuring that PHI is safeguarded, not only in the Company's computer systems and filing cabinets, but in every way that we use and share it."[18]

39. Dominion National maintains a "Notice of Privacy Practices" that similarly expressly promises to protect customer PHI and states that it is "***legally required*** to follow the privacy practices that are described in this notice." [19] Indeed, Dominion National expressly acknowledges "***Our Legal Duty to Protect the Privacy of Your PHI***" which includes information it created or received about "past, present, or future health or condition," "the provision of health care services," payment for health care services, and identifying information such as "name, address, contract identification number, etc."

40. Dominion National claims that "one of our primary goals is to safeguard your PHI. We have policies and procedures in place throughout our organization to protect your information. These policies and procedures include: training all employees on appropriate uses, disclosures, and protection of PHI; limiting employee system access to only the PHI needed to

[18] *Id.*

[19] DOMINION NATIONAL, NOTICE OF PRIVACY PRACTICES (2018), (available at https://dominionnational.com/files/Privacy_Policy_Forms/DN_Privacy%20Notice.pdf) (emphasis added).

perform job duties; ensuring secure disposal of confidential information; using unique user IDs and passwords, etc. This protection covers oral, written, and electronic forms of PHI."

41. Dominion National's "Notice Concerning Financial Information" makes similar security promises "to protect your personal financial information." Specifically, Dominion National states that "we maintain physical, electronic, and procedural safeguards that comply with legal requirements to protect your personal financial information."[20]

42. Finally, Dominion National publishes a "Computer Use and Information Security" policy on its website.[21] "This policy assists Dominion in providing a business aligned security program that meets its operational, compliance, and information security needs to protect the confidentiality, integrity, and availability of information, data, and the supporting systems."

43. The Computer Use and Information Security Policy defines "Confidential Information" as "information prepared, generated, received, and/or maintained in written or electronic form by Dominion with the expectation of Dominion and/or other party (e.g., members, provider, or employer) that the information will be kept private and will not be disclosed to unauthorized parties." It also recognizes and defines Protected Health Information (PHI) as "individually identifiable health information which is transmitted or maintained in any form (verbal, paper, electronic) which can be used to identify an individual who has Dominion's coverage.

44. The Computer Use and Information Security Policy sets forth generic policies

[20] DOMINION NATIONAL, NOTICE CONCERNING FINANCIAL INFORMATION (2018), (available at https://dominionnational.com/files/Privacy_Policy_Forms/DN_GLB.pdf)

[21] DOMINION NATIONAL, COMPUTER USE AND INFORMATION SECURITY, (2018) (available at https://dominionnational.com/files/Privacy_Policy_Forms/IT-110%20Computer%20Use%20and%20Information%20Security%20Policy.pdf)

and guidelines for information access, workstation use, device and media control, virus and malicious software protection, e-mail and the internet, remote access, security awareness, reporting incidents, and violations of the policy. In relevant part the Policy provides that:

- "Access to computing facilities, and the information residing on computing facilities, must be limited to the level of access that is needed by an individual to perform his or her job functions. Individuals may not seek or be given access privileges beyond the reasonable minimum necessary access needed to perform their job function."
- "Access to computing facilities and information must be controlled through the use of an individually owned unique user ID and associated confidential password or other approved authentication method. This password is used to authenticate the owner of the user ID and must never be shared with anyone."
- "The IT Department is tasked with the completion of regular access and role reviews on applications and platforms it deems appropriate."
- "All individuals are also responsible for protecting computer resources from unauthorized use."
- "PHI and other sensitive information must be removed from electronic media and/or devices when the asset or media is no longer needed and/or when the media will no longer be under corporate control. . . . The removal of this information must be followed by an approved overwrite operation using the data destruction utility specifically designed for this purpose. If this is not possible, the physical destruction of the media is required to insure the confidentiality of the information."

- "Storage or duplication of PHI or other corporate critical information on portable media should be performed only where there is a business need. Appropriate controls must be used to ensure the data is protected, such as encryption technology. Data placed on portable media must be logged and a copy retained."
- "All computer devices must utilize anti-virus and malware software where appropriate. The software must: [1] Be enable at all times[;] [2] Scan for viruses and malware on a regular basis, in accordance with corporate guidelines[;] [3] Have pattern files updated in accordance with corporate guidelines[;] [and 4] Have on-access scanning enabled to ensure that any external files are scanned before being introduced into corporate computers.
- "PHI and other sensitive information must not be sent outside the company unless it has been secured and is being sent to an authorized individual . . . . Information that is attached to e-mail must be scanned for viruses before being introduced into, or before leaving, the corporate computing environment . . . . [and] Access to the Internet must pass through a controlled corporately recognized environment."
- "The only approved method of remotely accessing the corporate computing environment is through the use of the standard corporate solutions. Dominion's IT Strategy, for use by the IT Department, contains additional information about remote access. The establishment of and or use of unauthorized remote access methods or technologies are expressly prohibited."
- "All existing members of the workforce are required to pass a Security

Awareness training program, be aware of security policies, and understand the reasons why policies and procedures are in place. Workforce members must stay informed about their ongoing responsibilities, especially those related to securing PHI and other sensitive information."

- "All users of Dominion's systems must report any unusual computer activity such as a perceived virus, an authorized access or use event, or loss or theft of Dominion equipment (e.g. laptop or mobile device), by submitting an IT Help Desk Ticket . . . . Further, disclosures of PHI should be reported to Dominion's Compliance/Privacy Office in accordance with the Guidelines When Filling Out Disclosure Forms. The Privacy Officer will coordinate with IT, and vice versa, concerning information security and privacy matters."
- "Individuals who suspect, or have knowledge of a violation of an information security policy must report that violation immediately to their manager/supervisor. The manager/supervisor should evaluate the information and contact IT Management if it appears that a violation has occurred."

45. The Computer Use and Information Security Policy references the "Dominion Information Security Strategy" for "IT Department use" which is not available publicly online. It likewise refers to "HR-0735, Privacy of Member Information" which is not available to the public.

46. Despite these promises to safeguard the millions of customers' sensitive and confidential information in its possession, Dominion National failed to implement adequate security protocols and measures to ensure that it met these obligations. Instead, Dominion National chose to avoid making the security infrastructure and personnel investments necessary

to prevent, detect, and remove unauthorized users from the databases where it stored confidential patient information.

47. Dominion National should have known better. Particularly in light of the massive data breaches at other health insurance companies, Dominion National should have devoted more resources to data security.

D. Providence Health Plan contracted with Dominion National for dental plan administration benefits without adequately investigating Dominion National's ability to protect its Members' sensitive information.

48. Providence Health Plan is an insurance provider offering insurance plans and benefits in the State of Oregon. Providence Health Plan contracted with Dominion National to administer its dental benefits starting on January 1, 2015.[22] At the time, Providence Health Plan provided health care coverage services to more than 460,000 individuals in Oregon, Washington and Alaska.[23] When Providence Health Plan partnered with Dominion National, its customers expected that Dominion National would safeguard their confidential information provided through Providence Health Plan.

49. Like Dominion National, Providence Health Plan maintains its own security and confidentiality policies.

50. Providence Health Plan's "Confidentiality of Member Information" notice recognizes the importance of keeping confidential patient information secure: "Medical care is a deeply personal issue for people. All of us need to know that information about our health care is private and confidential. Providence Health Plan respects the privacy of our members and takes great care to determine when it is appropriate to share your personal health

[22] DOMINION NATIONAL, *Providence*, https://dominionnational.com/providence

[23] DOMINION NATIONAL, *Providence Health Plan Offers Dental Benefits with Dominion Dental Partnership*, https://dominionnational.com/news/2014-08-14

information."[24]

51. In its Notice of Privacy Practice, Providence Health Plan states, "we respect the privacy and confidentiality of your protected health information (PHI). We are required by law to maintain the privacy of your protected health information, (commonly called PHI or your personal information) including in electronic format. When we use the term 'personal information' we mean information that identifies you as an individual such as your name and Social Security Number, as well as financial, health and other information about you that is nonpublic, and that we obtain so we can provide you with insurance coverage. Providence Health Plan maintains policies that protect the confidentiality of personal information, including Social Security numbers, obtained from its members in the course of its regular business functions. We must provide you with this notice, and abide by the terms of this notice."[25]

52. Providence Health Plan discloses that it "may use or disclose your PHI with individual[s] who perform business functions on our behalf or provide use with services if the information is necessary for such functions or services." But promises that "our business associates are required, under contract with us and pursuant to federal law, to protect the privacy of your information and are not allowed to use or disclose any information other than as specific in our contract and as permitted by federal law."

53. Providence Health Plan could not have adequately vetted Dominion National's security to ensure that it complied with its own standards and promises to its customers before

[24] PROVIDENCE HEALTH PLAN, *Confidentiality of Member Information*, https://healthplans.providence.org/about-us/privacy-notices-policies/confidentiality-of-member-information/

[25] PROVIDENCE HEALTH PLAN, *Notice of privacy practices*, https://healthplans.providence.org/about-us/privacy-notices-policies/notice-of-privacy-practices/

entering into a contract with Dominion National to provide dental plan benefits administration. If Providence Health Plan had adequately investigated Dominion National's security policies, procedures, protections and infrastructure, it would have learned that it was woefully inadequate to protect the confidential personal and health information of its customers.

E. Dominion National's woefully inadequate data security resulted in a massive, nearly decade-long breach of its systems.

54. Dominion National failed to meet its obligations and promises to adequately secure confidential PII and PHI in its care.

55. On April 17, 2019, Dominion National received "an internal alert" which prompted it to retain FireEye Mandiant ("Mandiant") to conduct an investigation.[26]

56. On April 24, 2019, Dominion National determined, based on Mandiant's investigation, "that an unauthorized party may have accessed some of [its] computer servers. The unauthorized access may have occurred as early as August 25, 2010" ("Data Breach"). [27]

57. The fact that this Data Breach went undetected for nearly a decade indicates that Dominion National's data security measures were woefully inadequate and failed to comply with evolving industry-standard practices. Data security programs, standards, and protocols are constantly improving. The fact that hackers remained undetected in Dominion National's servers for nine years indicates that Dominion National failed to update or replace hardware, failed to update or install software designed and restrict intrusions into protected databases, did not have a Security Incident & Event Management (SIEM) system in place to identify and monitor IT-security events in real time, did not have logs or failed to monitor its logs of remote

[26] MARYLAND HEALTH CONNECTION, *Dominion Dental reports data security breach*, https://www.marylandhealthconnection.gov/dominion-dental-reports-data-security-breach/

[27] DOMINION NATIONAL FACTS, *A message from Dominion National President, Mike Davis*, https://dominionnationalfacts.com/index.html

access to its networks, failed to conduct regular internal and external security audits, failed to conduct penetration tests to determine and correct weaknesses in its security systems, failed to install or adequately implement the anti-malware and anti-virus software it referenced in its security policies, and generally failed to comply with industry-standard security protocols and processes.

58. On June 21, 2019, Dominion National issued a press release and launched a website notifying its customers about the breach.[28]

59. Dominion National claimed to have reviewed the data stored and potentially accessed during this breach and "determined that the data may include enrollment and demographic information for current and former members of Dominion National and Avalon vision, and current and former members of plans we provide administrative services for. In addition, the data may include personal information for producers who placed Dominion National and Avalon vision policies, and healthcare providers participating in the insurance programs of Dominion National. The member information may have included names, addresses, email addresses, dates of birth, Social Security numbers, member ID numbers, group numbers, and subscriber numbers. For members who enrolled online through Dominion National's website, their bank account and routing numbers may have also been included in the data. The provider information may have included names, dates of birth, Social Security numbers, and/or taxpayer identification numbers. The producer information may have included names and Social Security numbers."[29]

60. Dominion National claims that "it moved quickly to clean the affected servers

[28] *Id.*

[29] *Id.*

and implement enhanced monitoring and alerting software. Dominion National also contacted the FBI and will continue to work with them during their investigation. Dominion National has no evidence that any information was in fact accessed, acquired, or misused."[30]

61. Providence Health Plan also issued a notice on its webpage. It states that "On June 21, 2019, Providence Health Plan was notified by a business associate of a privacy incident involving health plan member information. The incident involved the potential unauthorized access of computer servers at Dominion National. Dominion National is a company that provides Providence Health Plan with administration of dental benefits."[31]

62. Providence Health Plan informed its members that "the data stored or potentially accessible from Dominion National's computer servers may have included enrollment and demographic information for current and former members of Providence Health Plan's dental program. The information may include names, addresses, email addresses, dates of birth, Social Security numbers, member identification numbers, group numbers and subscriber numbers."[32]

63. Industry reporters have indicated that as many as 2,964,667 individuals may have had their data exposed and stolen in this data breach.[33]

64. Dominion National began mailing notices to affected consumers on June 21, 2019.

65. Two months after it alerted its own customers, Dominion National alerted Providence Health Plan subscribers of that breach. In an August 20, 2019 letter, Dominion

---

[30] DOMINION NATIONAL FACTS, *Frequently Asked Questions*, https://dominionnationalfacts.com/faq.html

[31] PROVIDENCE HEALTH PLAN, *Providence Health Plan member notification*, https://healthplans.providence.org/about-us/news-notices-announcements/member-notification/

[32] *Id.*

[33] HIPAA JOURNAL, *June 2019 Healthcare Data Breach Report*, HTTPS://www.hipaajournal.com/june-2019-healthcare-data-breach-report/

National claimed that "we recently identified and addressed a data security incident at Dominion National that may have involved your information. This incident was isolated to Dominion National's systems and did not affect Providence Health Plan."

66. Dominion National, however, failed to inform Providence Health Plan consumers what specific data of theirs was compromised. Instead, the letter identified the accessed information as general "enrollment and demographic information for current and former members of Providence Health Plan's dental program. This information may include your name, address, e-mail address, date of birth, Social Security number, member ID number, group number, and subscriber number."

67. The letter "encouraged" members "to remain vigilant for incidents of fraud by monitoring your insurance statements and explanations of benefits" and also recommended that recipients "monitor your financial account statements." But without knowing what data was specifically compromised, affected individuals could not take any specific steps to preemptively mitigate identity theft, or the misuse of their financial information or medical information.

G. Plaintiff's Specific Allegations

68. Plaintiff Mark Bradley is a resident of Portland, Oregon. He was insured by Providence Health Plan through his insurer from 2015 until 2019. During this time, Providence Health Plan contracted with Dominion National to administer the dental benefits under Mr. Bradley's insurance plan.

69. Mr. Bradley's personal and medical information was provided to Dominion National through Providence Health Plan and dental care providers. Mr. Bradley received dental care on numerous occasions during the four years his dental benefits were administered

by Dominion National.

70. Mr. Bradley received a letter dated August 20, 2019 informing him that his information may have been compromised in the Dominion National Data Breach. This letter did not, however, inform him what information was compromised or located on the affected servers.

71. Prior to the Data Breach, Mr. Bradley had taken care to ensure that his personal information is not exposed to malicious actors. The hackers who breached Dominion National's servers intentionally targeted the personal, financial, and health information of individuals like Mr. Bradley. Mr. Bradley is extremely distraught that his careful efforts to protect his personal, confidential data have been thwarted by the misconduct of Dominion National. As a result of the Data Breach, Mr. Bradley has devoted time and effort to monitoring his financial and medical accounts. Due to the confidential nature of the information provided to Dominion National, Mr. Bradley has a substantial and imminent future risk of harm, including identity theft and medical fraud.

72. Mr. Bradley has been harmed in that he failed to receive the benefit of his bargain. Mr. Bradley has further been harmed in that the value of his private information has been lessened.

H. Plaintiff and Class Members have been harmed by the Data Breach.

73. Plaintiff Mark Bradley and the Class Members he seeks to represent have been harmed by the Data Breach. Class Members had a reasonable expectation that Dominion National—pursuant to its legal obligations and express promises—would protect the confidential PII and PHI the provided to Dominion National in exchange for services.

74. Dominion National breached its duties and obligations to Plaintiff and all Class

Members by failing to maintain adequate data security to protect the confidential PII and PHI in its possession.

75. As a result of the Data Breach, Plaintiff and Class Members have a substantial and imminent risk of suffering from identity theft and financial and medical fraud. Plaintiff and Class Members have suffered actual damages, including ongoing, imminent, and certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their personal information; lost value of the benefit of their bargain; and other economic and non-economic harm.

CLASS ACTION ALLEGATIONS

76. Plaintiffs bring this action on behalf of a Nationwide Class, Oregon Subclass, and Providence Health Plan Subclass as defined as follows:

a. Nationwide Class: All individuals in the United States whose Personal Information was compromised as a result of the data breach announced by Dominion National on or about June 21, 2019.

b. Oregon Subclass: All individuals in the State of Oregon whose Personal Information was compromised as a result of the data breach announced by Dominion National on or about June 21, 2019.

c. Providence Health Plan Subclass: All individuals insured by Providence Health Plan at any time between January 1, 2015 to April 24, 2019 whose dental plan benefits were administered by Dominion National and whose information was compromised as a result of the data breach announced by Dominion National on or about June 21, 2019.

77. To the extent necessary for manageability, Plaintiffs propose, in the alternative to the Nationwide Class, that the Court certify state subclasses in order to group similar causes of action for states requiring similar evidentiary proof, defined as follows:

a. Alternative Statewide Subclasses: All individuals in the State of [insert State name] whose personal Information was compromised as a result of the data breach announced by Dominion National on or about June 19, 2019.

78. Plaintiff reserves the right to amend the Class definitions if discovery and further investigation reveal that the Classes should be expanded, divided into further subclasses or modified in any other way. Plaintiff reserves the right to propose other subclasses prior to trial.

79. Excluded from the Class and Subclasses are Defendants, and their parents, subsidiaries, agents, officers and directors. Also excluded is any judicial officer assigned to this case and members of his or her staff.

80. Plaintiff seeks class certification pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3). In the alternative, Plaintiff seeks class certification under Fed. R. Civ. P. 23(c)(4) because the common questions listed herein predominate as to particular issues that could substantially advance the litigation. The proposed classes and subclasses meet the applicable requirements for certification under Fed. R. Civ. P. Rule 23.

81. **Numerosity**: The exact number of members of the Classes is unknown to Plaintiffs at this time, but on information and belief, there are likely over a million class members, making joinder of each individual member impracticable. Ultimately, members of the Classes will be easily identified through Defendants' records.

82. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include, but are not limited to:

a. Whether Dominion National failed to safeguard Plaintiffs' and the Classes' sensitive information adequately;

b. Whether Dominion National failed to protect or otherwise keep Plaintiffs' and the Classes' sensitive information secure, as promised;

c. Whether Dominion National failed to maintain adequate privacy and security safeguards;

d. Whether Dominion National's data security complied with relevant industry and government standards;

e. Whether Dominion National acted negligently in failing to secure and safeguard Plaintiffs' and Class Members' data;

f. Whether Class Members have implied contracts with Dominion National;

g. Whether Dominion National breached any implied contracts with Class Members;

h. Whether Class Members have third-party beneficiary status under the contract(s) between Dominion National and Providence Health Plan;

i. Whether Dominion National breached its contract with Providence Health Plan;

j. Whether Defendants' conduct entitles Class Members to damages or restitution, and if so, in what amount; and

k. Whether injunctive relief is appropriate to ensure the future privacy and security of Class Members' personal information.

83. **Typicality**: Plaintiff's claims are typical of the claims of the members of the Classes. Plaintiff and the members of the Classes sustained damages as a result of Defendants' uniform wrongful conduct during transactions with them.

84. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Classes, and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Classes, and Defendants have no defenses unique to Plaintiff. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Classes, and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Classes.

85. **Risks of Prosecuting Separate Actions**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendants or would be dispositive of the interests of members of the proposed Classes.

86. **Policies Generally Applicable to the Classes**: This class action is appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Plaintiff and proposed Classes as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the

Classes, and making final injunctive relief appropriate with respect to the proposed Classes as a whole. Defendants' practices challenged herein apply to and affect the members of the Classes uniformly, and Plaintiff's challenge of those practices hinges on Defendants' conduct with respect to the proposed Classes as a whole, not on individual facts or law applicable only to Plaintiff.

87. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Classes. The injuries suffered by each individual member of the Classes are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendants' conduct. Absent a class action, it would be virtually impossible for individual members of the Classes to obtain effective relief from Defendant. Even if members of the Classes could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court. Requiring individual Class Members to seek relief on their own would be prohibitively costly to all parties, including Defendants, and overburden the court system.

FIRST CAUSE OF ACTION
NEGLIGENCE against DOMINION NATIONAL DEFENDANTS
(On behalf of Plaintiff and the Nationwide Class or, in the alternative, the Oregon Subclass)

88. Plaintiff realleges and incorporates all previous paragraphs as though fully set forth herein.

89. The Dominion National Defendants required Plaintiff and other Class Members to provide sensitive, non-public personal, financial and medical information in order to obtain insurance services or to administer insurance benefits.

90. By collecting and storing this data for many years, Dominion National had a duty of care to use reasonable means to secure and safeguard this information and ensure its privacy and confidentiality, to prevent disclosure of this information to unauthorized persons, to guard the information from unauthorized access, to protect the information from theft, to comply with industry-standard data security practices, to comply with federal law governing the protection of PHI, and to comply with its own privacy and security policies, among other duties.

91. Dominion National assumed a duty of care to use reasonable means to implement policies and procedures to prevent unauthorized disclosure of sensitive PII and PHI.

92. Dominion National breached this duty of care by failing to implement policies and procedures to prevent unauthorized disclosure and theft of this personal information.

93. Dominion National breached this duty of care by failing to adequately safeguard the privacy, confidentiality, and security of Plaintiff's and Class Members' PII and PHI.

94. Dominion National knew or should have known that Plaintiff's and Class Members' PII and PHI were valuable on the dark web and therefore that it was a particular target of malicious actors seeking to obtain that information for financial gain or other nefarious purposes.

95. Given the publicly available and highly publicized knowledge that health insurance companies were a target of cybercriminals, Plaintiff and Class Members are part of a well-defined, foreseeable, finite and discernible group that was at high risk of having their PII

and PHI misused if disclosed or not protected by Dominion National.

96. Dominion National breached its common law, statutory, and other duties—and thus, were negligent—by failing to use reasonable measures to adequately protect consumers' PII and PHI from exposure to unauthorized third parties, failing to limit the severity of the exposure, and failing to detect the exposure in a timely fashion.

97. It was therefore reasonably foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII and PHI would result in one or more of the following injuries to Plaintiff and Class Members: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing insurance statements, bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the sensitive information, and other economic and non-economic harm.

98. Plaintiff and Class Members have suffered actual damages and are entitled to injunctive relief and monetary relief in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE against DOMINION NATIONAL DEFENDANTS
(On behalf of Plaintiff and the Nationwide Class, or in the alternative, the Oregon Subclass and Statewide Subclasses)

99. Plaintiff realleges and incorporates all previous paragraphs as though fully set forth herein.

100. As a health insurance provider and benefits administrator, Dominion National is

an entity covered by HIPAA, 45 C.F.R. § 160.102. Dominion National is therefore obligated to comply with all rules and regulations under 45 C.F.R. Part 160 and 164.

101. 45 C.F.R. Part 164 governs "Security and Privacy", with Subpart A providing "General Provisions," Subpart B regulating "Security Standards for the Protection of Electronic Protected Health Information," Subpart C providing requirements for "Notification in the Case of Breach of Unsecured Protected Health Information," and Subpart E governing "Privacy of Individually Identifiable Health Information."

102. 45 C.F.R. § 164.104 states that the "standards, requirements, and implementation specifications adopted under this part" apply to covered entities and their business associates, such as Dominion National.

103. Dominion National is obligated under HIPAA to, among other things, "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits" and "protect against any reasonably anticipated threats or hazards to the security or integrity of such information." 45 C.F.R. § 164.306.

104. 45 C.F.R. Sections 164.308 (Administrative safeguards), 164.310 (Physical safeguards), 164.312 (Technical safeguards), 164.314 (Organizational requirements), and 164.316 (Policies and procedures and documentation requirements) provide mandatory standards that all covered entities must adhere to.

105. Dominion National violated HIPAA by failing to adhere to and meet the required standards as set forth in 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

106. Plaintiff and Class Members fall within the class of persons HIPAA and its

implementing regulations were designed to protect and the harm suffered was the type of harm HIPAA and its implementing regulations were designed to prevent.

107. Dominion National's violations of HIPAA regulations constitutes negligence per se.

108. Likewise, HIPAA regulations require covered entities to "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach" "notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of" a data breach. 45 C.F.R. § 164.404. The notice must also contain a minimum amount of information regarding the breach (including the dates of the breach and its discovery), the types of protected health information that were involved, steps individuals should take to protect themselves from harm resulting from the breach, a description of what the entity is doing to investigate the breach and mitigate harm, and contact information to obtain further information. *Id.*

109. Dominion National breached its notification obligations under HIPAA by failing to give adequate and timely notice of the breach to Plaintiff and Class Members.

110. Plaintiff and Class Members fell within the class of persons the HIPAA notification regulations were designed to protect and the harm suffered was the type of harm HIPAA was required to prevent.

111. Dominion National's inadequate and untimely notification constitute negligence per se.

112. Section 5 of the Federal Trade Commission Act ("FTCA") also prohibits "unfair or deceptive acts or practices in or affecting commerce." 45 U.S.C. § 45(a)(1). The Federal Trade Commission has interpreted this provision to include failure to use reasonable measures

to protect PII.

113. Dominion National violated the FTCA by failing to implement and use reasonable measures to protect Plaintiff and Class Members' personal information, including not adhering to industry standards. Dominion National's conduct was unreasonable and unfair in light of the nature of the information its obtained and stored in the regular course of its business—confidential personal, financial, and medical information—and the consequences of failing to adequately protect such information were foreseeable. The data breach and the damages suffered by Plaintiff and Class Members as a result were reasonably foreseeable.

114. Plaintiff and Class Members fall within the class of persons the FTCA is designed to protect and the harms they have and will suffer are those which the FTCA is designed to prevent.

115. Dominion National's violations of the FTCA constitute negligence per se.

116. As a result of Dominion National's negligence per se in violating HIPAA and the FTCA, Plaintiff and Class Members have suffered and will continue to suffer actual damages.

117. Plaintiff and Class Members have suffered actual damages and are entitled to injunctive relief and monetary relief in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF CONTRACT against DOMINION NATIONAL DEFENDANTS
(On behalf of Plaintiff and the Nationwide Class, or in the alternative, the Oregon Subclass and Statewide Subclasses)

118. Plaintiff realleges and incorporates all previous paragraphs as though fully set forth herein.

119. Dominion National maintained its "Notice of Privacy Practices," "Notice Concerning Financial Information" and "Computer Use and Information Security Policy" on its

website and which individually and collectively constituted one or more agreements between Dominion National and persons who provided their personal information to Dominion National, including Plaintiff and Class Members.

120. Plaintiff and Class Members performed under the agreement when they provided their personal information subject to these agreements to Dominion National in exchange for insurance coverage and/or plan administration services.

121. These Notices and Policies obligated Dominion National to undertake certain data security protections and protocols to safeguard Plaintiff's and Class Members' information.

122. Plaintiff and Class Members were also third-party beneficiaries of Dominion National's "Code of Conduct" which applies to Dominion National's employees, officers, committee members, and directors.

123. The "Code of Conduct" was implemented for the express benefit of individuals who are current or former members of Dominion National's insurance plans and current and former members of insurance plans whose dental and/or vision benefits were administered by Dominion National. The Code of Conduct required Dominion National and its employees, officers, committee members, and directors to ensure the privacy of confidential information provided by customers.

124. Dominion National breached its obligations under each of these agreements when it failed to implement adequate data security measures.

125. Plaintiff and Class Members' were injured as a direct and proximate result of Dominion National's breach of the Notice of Privacy Practices, Notice Concerning Financial Information, Computer Use and Information Security Policy and Code of Conduct.

126. Plaintiff and Class Members suffered actual damages as a result of Dominion National's breach of contract and are entitled to injunctive relief and monetary relief in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
BREACH OF CONTRACT AS THIRD PARTY BENEFICIARY against DOMINION NATIONAL DEFENDANTS
(On behalf of Plaintiff and the Providence Health Plan Subclass)

127. Plaintiff realleges and incorporates all previous paragraphs as though fully set forth herein.

128. Providence Health Plan entered into a contract with Dominion National to administer its dental benefits for its insureds.

129. On information and belief, this contract required Dominion National to implement, utilized, and maintain reasonable and adequate data security measures to protect Providence Health Plan's Members' confidential personal, financial, and medical information.

130. Plaintiff and Providence Health Plan Subclass Members were the intended beneficiaries of this agreement between Providence Health Plan and Dominion National.

131. Dominion National breached its agreement with Providence Health Plan by failing to implement, utilize and maintain reasonable and adequate data security measures to protect Providence Health Plan Subclass Members' data from unauthorized disclosure.

132. Plaintiff and Providence Health Plan Subclass Members were harmed as a direct and proximate result of Dominion National's breach of contract.

133. Plaintiff and Providence Health Plan Subclass Members suffered actual damages as a result of Dominion National's breach of contract and are entitled to injunctive relief and monetary relief in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
BREACH OF CONTRACT against PROVIDENCE HEALTH PLAN
(On behalf of Plaintiff and the Providence Health Plan Subclass)

134. Plaintiff realleges and incorporates all previous paragraphs as though fully set forth herein.

135. Providence Health Plan maintains a "Notice of Privacy Practice" which constitutes a contract between Providence Health Plan and its members.

136. Plaintiff and Providence Health Plan Subclass Members performed under this Agreement when they provided Providence Health Plan their confidential information subject to this agreement.

137. In its Notice of Privacy Practice, Providence Health Plan promises that it "may use or disclose your PHI with individual who perform business functions on our behalf or provide use with services if the information is necessary for such functions or services." But promises that "our business associates are required, under contract with us and pursuant to federal law, to protect the privacy of your information and are not allowed to use or disclose any information other than as specific in our contract and as permitted by federal law."

138. Providence Health Plan entered into a contract with Dominion National to provide dental benefits administration services for its Members.

139. Providence Health Plan breached its promise to its Members when it entered into the contract with Dominion National because Dominion National did not have adequate security measures to protect the privacy of Plaintiff and Providence Health Plan Subclass Members' data.

140. Plaintiff and Providence Health Plan Subclass Members were harmed as a direct and proximate result of Providence Health Plan's breach of contract.

141. Plaintiff and Providence Health Plan Subclass Members suffered actual damages as a result of Dominion National's breach of contract and are entitled to monetary relief in an amount to be proven at trial.

SIXTH CAUSE OF ACTION
NEGLIGENCE against PROVIDENCE HEALTH PLAN
(On behalf of Plaintiff and the Providence Health Plan Subclass)

142. Plaintiff realleges and incorporates all previous paragraphs as if fully set forth herein.

143. Providence Health Plan shares confidential and protected personal information of its Members with other companies under limited circumstances as permitted by law. Providence Health Plan shared confidential and protected information of its Members with Dominion National as part of Dominion National's provision of dental plan administration services.

144. Providence Health Plan had a duty of care to ensure that any business associates, such as Dominion National, to which it provided confidential Member information had and maintained adequate data security measures to protect such data.

145. Providence Health Plan had a duty of care to conduct a sufficient investigation into the security practices, protocols and protections of any business associate, such as Dominion National, to which it provided confidential and protected Member information.

146. Providence Health Plan breached its duty of care by failing to conduct an adequate investigation into Dominion National's data security practices and by providing Dominion National with Plaintiff and Providence Health Plan Subclass Members' personal information.

147. Providence Health Plan knew or should have known that Dominion National did

not have adequate data security measures in place to protect Plaintiff and Providence Health Plan Subclass Members' personal information, yet provided it anyway.

148. Providence Health Plan knew that Plaintiff and Providence Health Plan Subclass Members' personal information was valuable on the dark web and therefore that Dominion National was a potential target of cybercriminals seeking to obtain that information for financial gain or other nefarious purposes.

149. Given the publicly available and highly publicized knowledge that health insurance companies were a target of cybercriminals, Plaintiff and Providence Health Plan Subclass Members are part of a well-defined, foreseeable, finite and discernible group that was at high risk of having their PII and PHI misused if disclosed or not protected by the companies Providence Health Plan shared it with.

150. It was therefore reasonably foreseeable that Providence Health Plan's failure to adequately investigate the security practices and measures in place at Dominion National before entering into a contract for dental plan administration services and providing protected information to Dominion National would result in injury to Plaintiff and the Providence Health Plan Subclass.

151. Plaintiff and the Providence Health Plan Subclass members have suffered actual damages and are entitled to monetary relief in an amount to be proven at trial.

REQUEST FOR RELIEF

Plaintiff, individually and on behalf of members of the Class and Subclasses, as applicable, requests that the Court enter judgment in his favor and enter and Order or Orders as follows:

1. Certifying this case as a class action on behalf of Plaintiff and the Classes and

Subclasses as defined above, appointing Plaintiff as representative of the appropriate Classes, and appointing the undersigned attorneys as Lead Class Counsel;

2. Finding that Defendants' actions, as described above, constitutes negligence, negligence per se, and breach of contract.

3. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Classes, including, but not limited to, an order (i) prohibiting Defendants from engaging in the wrongful and unlawful acts described here, and (ii) requiring Defendants to safeguard the privacy, confidentiality and security of Plaintiff's and Class Members' personal information collected in the course of its business in accordance with federal, state, and local laws and regulations, and industry standards; (iii) requiring Defendants to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing to determine any further vulnerabilities to Class Members' personal information; and (iv) ordering Defendants to implement new data storage and management protocols that adequately protect the privacy, confidentiality and security of Plaintiffs and Class Members' personal information.

4. Awarding actual, statutory, exemplary and punitive damages to Plaintiffs and the Class, where applicable, in an amount to be determined at trial;

5. Awarding Plaintiffs and the Classes their reasonable litigation expenses and attorneys' fees;

6. Awarding Plaintiffs and the Classes pre- and post-judgment interest, to the extent allowable;

7. Permitting Plaintiffs and the Classes to amend their pleadings to conform to the evidence produced at trial; and

8. Awarding such other and further relief as equity and justice may require.

JURY DEMAND

Plaintiff requests a trial by jury.

DATED: September 17, 2019

Respectfully submitted,

/s/ *Bernard J. DiMuro, Esq.*
Bernard J. DiMuro (VSB No. 18784)
DIMUROGINSBERG, P.C.
1101 King Street, Suite 610
Alexandria, Virginia 23314
(703) 684-4333
Fax: (703) 548-3181
Email: bdimuro@dimuro.com

Kim D. Stephens*
Jason T. Dennett*
Rebecca Solomon*
TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
(206) 682-5600
Fax: (206) 682-2992
Email: kstephens@touslev.com
Email: jdennett@touslev.com
Email: rsolomon@tousley.com

Walter D. Kelley, Jr. (VSB No. 21622)
James Pizzirusso (VSB No. 47296)
HAUSFELD LLP
1700 K Street NW, Suite 650
Washington, DC 20006
(202) 540-7200
Fax: (202) 540-7201
Email: wkelley@hausfeld.com
Email: jpizzirusso@hausfeld.com

Andrew Friedman*
Douglas J. McNamara*
Karina Puttieva*
Paul Whalen*
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue, NW, Suite 500
Washington, DC 20005
(202) 408-4600
Fax: (202) 408-4699
Email: afriedman@cohenmilstein.com
Email: dmcnamara@cohenmilstein.com
Email: kputtieva@cohenmilstein.com
Email: pwhalen@cohenmilstein.com

Counsel for Plaintiffs and the Class

**Pro Hac Vice Applications to be Submitted*

JS 44 (Rev. 12/07)

CIVIL COVER SHEET

Attachment 2

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON THE REVERSE OF THE FORM.)

I. (a) PLAINTIFFS

Mark Bradley, individually and on behalf of all persons similarly situated

(b) County of Residence of First Listed Plaintiff Multnomah County, OR
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorney's (Firm Name, Address, and Telephone Number)
(see additional sheet)

DEFENDANTS

Dominion Dental Services USA, Inc., Dominion Dental Services, Inc., Capital Advantage Insurance Company, Capital Bluecross, and Providence Health Plan

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question (U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT (Place an "X" in One Box Only)

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excl. Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury

PERSONAL INJURY
- ☐ 362 Personal Injury - Med. Malpractice
- ☐ 365 Personal Injury - Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 444 Welfare
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 440 Other Civil Rights

PRISONER PETITIONS
- ☐ 510 Motions to Vacate Sentence

Habeas Corpus:
- ☐ 530 General
- ☐ 535 Death Penalty
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition

FORFEITURE/PENALTY
- ☐ 610 Agriculture
- ☐ 620 Other Food & Drug
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 630 Liquor Laws
- ☐ 640 R.R. & Truck
- ☐ 650 Airline Regs.
- ☐ 660 Occupational Safety/Health
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Mgmt. Relations
- ☐ 730 Labor/Mgmt.Reporting & Disclosure Act
- ☐ 740 Railway Labor Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Empl. Ret. Inc. Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 463 Habeas Corpus - Alien Detainee
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 810 Selective Service
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 875 Customer Challenge 12 USC 3410
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 892 Economic Stabilization Act
- ☐ 893 Environmental Matters
- ☐ 894 Energy Allocation Act
- ☐ 895 Freedom of Information Act
- ☐ 900Appeal of Fee Determination Under Equal Access to Justice
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN (Place an "X" in One Box Only)

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district (specify) ☐ 6 Multidistrict Litigation ☐ 7 Appeal to District Judge from Magistrate Judgment

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing **(Do not cite jurisdictional statutes unless diversity)**:
28 U.S.C. § 1332(d)

Brief description of cause:
Class Action Fairness Act of 2005

VII. REQUESTED IN COMPLAINT:

☑ CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ☑ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Brinkema DOCKET NUMBER 1:19-cv-1050

DATE 09/17/2019

SIGNATURE OF ATTORNEY OF RECORD /s/ Bernard J. DiMuro, Esq. (VSB No. 18784)

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

Attachment 2

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. (a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.C.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.

United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; federal question actions take precedence over diversity cases.)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerks in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the seven boxes.

Original Proceedings. (1) Cases which originate in the United States district courts.

Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.

Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

Multidistrict Litigation. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407. When this box is checked, do not check (5) above.

Appeal to District Judge from Magistrate Judgment. (7) Check this box for an appeal from a magistrate judge's decision.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity**. Example: U.S. Civil Statute: 47 USC 553
Brief Description: Unauthorized reception of cable service

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.

Demand. In this space enter the dollar amount (in thousands of dollars) being demanded or indicate other demand such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

PLAINTIFF'S ATTORNEY INFORMATION

Bernard J. DiMuro (VSB No. 18784)
DIMUROGINSBERG, P.C.
1101 King Street, Suite 610
Alexandria, Virginia 23314
(703) 684-4333
Fax: (703) 548-3181
Email: bdimuro@dimuro.com

Kim D. Stephens*
Jason T. Dennett*
Rebecca Solomon*
TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
(206) 682-5600
Fax: (206) 682-2992
Email: kstephens@touslev.com
Email: jdennett@touslev.com
Email: rsolomon@tousley.com

Walter D. Kelley, Jr. (VSB No. 21622)
James Pizzirusso (VSB No. 47296)
HAUSFELD LLP
1700 K Street NW, Suite 650
Washington, DC 20006
(202) 540-7200
Fax: (202) 540-7201
Email: wkelley@hausfeld.com
Email: jpizzirusso@hausfeld.com

Andrew Friedman*
Douglas J. McNamara*
Karina Puttieva*
Paul Whalen*
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue, NW, Suite 500
Washington, DC 20005
(202) 408-4600
Fax: (202) 408-4699
Email: afriedman@cohenmilstein.com
Email: dmcnamara@cohenmilstein.com
Email: kputtieva@cohenmilstein.com
Email: pwhalen@cohenmilstein.com

**Pro Hac Vice Applications to be Submitted*