IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE DOMINION DENTAL SERVICES USA, INC. DATA BREACH LITIGATION	Case No.: 1:19-cv-01050-LMB-MSN **JURY TRIAL DEMANDED**

FIRST CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Sayed Abubaker, Mark Bradley, Joseph Cardiff, Daniel W. Cho, Magdalyne Hilliard, and Matthew A. Slate (collectively, "Plaintiffs"), individually and on behalf of all persons similarly situated, bring this First Consolidated Class Action Complaint against Defendants Dominion Dental USA, Inc., Dominion Dental Services USA, Inc., Dominion Dental Services, Inc., Dominion National Insurance Company, and Dominion Dental Services of New Jersey, Inc. (together, "Dominion National"); Avalon Insurance Company ("Avalon"), Capital Advantage Insurance Company ("Capital Advantage"), Capital BlueCross (Dominion National, Avalon, Capital Advantage, and Capital BlueCross are referred to herein collectively as "Dominion Defendants"); and Providence Health Plan, based upon personal knowledge with respect to themselves, and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. Dominion National provides insurance and administrates dental and vision benefits offered by other insurers. Dominion Dental Services USA, Inc. administers the claims and benefits, and the other Dominion National defendants underwrite and issue insurance policies. Dominion Dental Services USA also administers claims and benefits for the insureds of other non-affiliated insurers. Dominion Dental USA provides additional administrative services to other defendants, including claims administration. On June 21, 2019, Dominion National announced that it was

subject to a massive data breach whereby the sensitive personal, financial, and medical information of nearly three million individuals was accessed as part of an ongoing, nine-year long data breach (the "Data Breach").

2. Beginning in August 2010 and continuing through April 2019, hackers exploited glaring vulnerabilities in Dominion National's databases to access the personal, financial, and medical information of current and former Dominion National members, and current and former members of other plans for which Dominion National provides administrative services. The stolen information includes names, addresses, email addresses, dates of birth, Social Security numbers, taxpayer identification numbers, member ID numbers, group numbers, subscriber numbers, and other protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and for members who enrolled online through Dominion National's website, bank account and routing numbers (collectively "Personal Information").

3. The Data Breach was discovered after Dominion National received an "internal alert" and retained cyber-security firm FireEye Mandiant to conduct an investigation. In a statement, Dominion National disclosed that, "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]

4. Dominion National is responsible for allowing the breach to occur by failing to

[1] Dominion National, Notice of Data Security Incident, https://dominionnationalfacts.com/ (last visited Nov. 22, 2019).

implement and maintain reasonable safeguards and failing to comply with industry-standard data security practices, contrary to the representations made in Dominion National's privacy statements and express and implied agreements with plan members and the insureds of third party insurers on whose behalf it provides benefit administration.

5. During the nine-year data breach period—one of the longest undiscovered breach periods ever—Dominion National failed to secure its databases containing massive amounts of members' Personal Information, failed to detect the hackers' presence, and failed to take any steps to investigate the numerous other red flags that should have warned the company that its systems were not secure. As a result of Dominion National's failure to protect the information they were entrusted to safeguard, Plaintiffs and Class Members did not receive the benefit of their bargains, and have been exposed to and are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future.

PARTIES

6. Plaintiff Sayed Abubaker is a resident and citizen of Washington, D.C., whose Personal Information was compromised in the Data Breach.

7. Plaintiff Mark Bradley is a resident and citizen of Portland, Oregon, whose Personal Information was compromised in the Data Breach.

8. Plaintiff Joseph Cardiff is a resident and citizen of New Kensington, Pennsylvania, whose Personal Information was compromised in the Data Breach.

9. Plaintiff Daniel WooHyun Cho is a resident and citizen of Johns Creek, Georgia, whose Personal Information was compromised in the Data Breach.

10. Plaintiff Magdalyne Hilliard is a resident and citizen of Mechanicsburg, Pennsylvania, whose Personal Information was compromised in the Data Breach.

11. Plaintiff Matthew A. Slate is a resident and citizen of Newport News, Virginia,

whose Personal Information was compromised in the Data Breach.

12. Defendant Dominion Dental USA, Inc., a Delaware corporation with its principal place of business in Arlington, Virginia, provides administrative services and certain management, human resources, corporate, legal, regulatory, and information systems services to other Dominion National Defendants. Dominion Dental USA, Inc. is a wholly-owned subsidiary of Capital Advantage Insurance Company, which is a wholly-owned subsidiary of Capital BlueCross.[2] Dominion Dental USA, Inc. is within the group of companies that utilize the name "Dominion National."

13. Defendant Dominion Dental Services USA, Inc., a Virginia corporation with its principal place of business in Arlington, Virginia, is a licensed administrator of dental and vision benefits. Dominion Dental Services USA, Inc. is a wholly-owned subsidiary of Dominion Dental USA, which is in turn a wholly-owned subsidiary of Capital Advantage Insurance Company, which is a wholly-owned subsidiary of Capital BlueCross. Dominion Dental Services USA, Inc. along with Dominion Dental Services, Inc. operates under the d/b/a "Dominion National."

14. Defendant Dominion Dental Services, Inc., a Virginia corporation with its principal place of business in Arlington, Virginia, is an insurance company that issues and underwrites dental plans in the District of Columbia, Delaware, Maryland, Pennsylvania, Virginia and New Jersey. Dominion Dental Services, Inc. is a subsidiary of Dominion Dental USA, which is a wholly-owned subsidiary of Capital Advantage Insurance Company, which is a wholly-owned subsidiary of Capital BlueCross. Dominion Dental Services, Inc. along with Dominion Dental Services USA, Inc. operates under the d/b/a "Dominion National."

[2] Examination Report of Dominion Dental Services, Inc. (December 31, 2016), https://www.scc.virginia.gov/boi/cons/fin/finex/95657.pdf (last visited Nov. 22, 2019).

15. Defendant Dominion National Insurance Company, a New Jersey company with its principal places of business in West Trenton, New Jersey and Arlington, Virginia, is an insurance company that underwrites dental and vision plans in New Jersey and Georgia. Dominion National Insurance Company is a subsidiary of Dominion Dental USA, which is a wholly-owned subsidiary of Capital Advantage Insurance Company, which is a wholly-owned subsidiary of Capital BlueCross. Dominion National Insurance Company is within the group of companies that utilize the name "Dominion National."

16. Defendant Dominion Dental Services of New Jersey, Inc., a New Jersey corporation with its principal place of business in Arlington, Virginia, is an insurance company that issues dental insurance plans in New Jersey. Dominion Dental Services of New Jersey is a subsidiary of Dominion Dental USA, which is wholly-owned subsidiary of Capital Advantage Insurance Company, which is a wholly-owned subsidiary of Capital BlueCross. Dominion Dental Services of New Jersey, Inc. is within the group of companies that utilize the name "Dominion National."

17. Defendant Avalon Insurance Company, a Pennsylvania company with its principal place of business in Harrisburg, Pennsylvania, is an insurance company that underwrites vision plans in Pennsylvania, Maryland, Delaware, Virginia, West Virginia and the District of Columbia. Dominion National's vision plans are underwritten by Avalon and administered by Dominion Dental Services USA, Inc. Avalon is a wholly-owned subsidiary of Capital Advantage Insurance Company, which is a wholly-owned subsidiary of Capital BlueCross.[3]

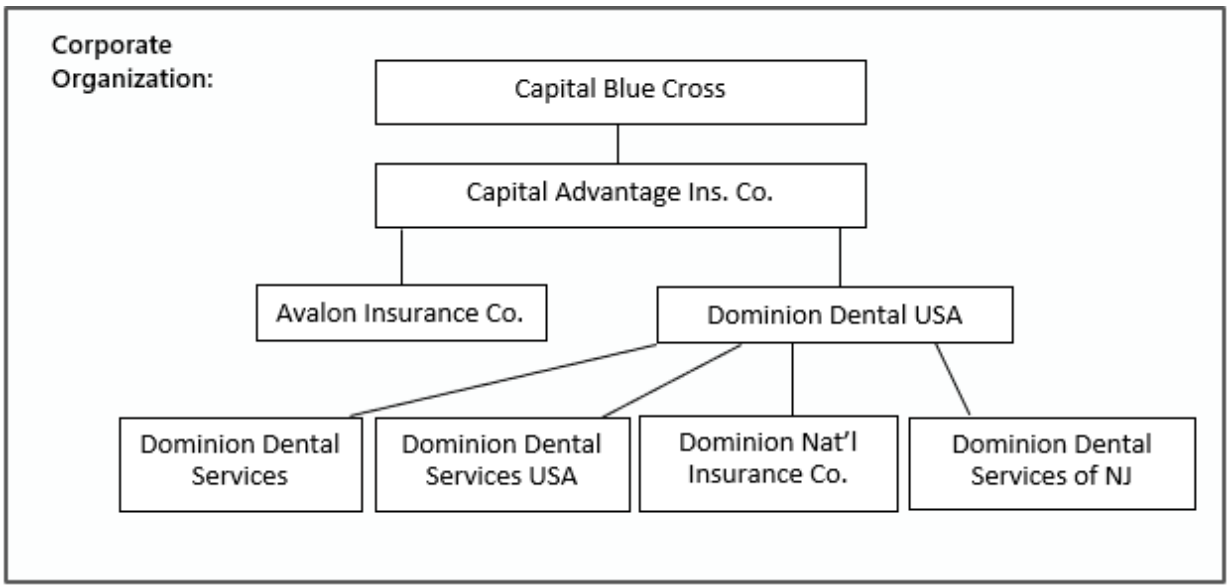
18. Defendant Capital Advantage Insurance Company, a Pennsylvania company with

[3] Report of Examination of Avalon Insurance Company (December 31, 2016), https://bit.ly/2TcuuQp (last visited Nov. 22, 2019).

its principal place of business in Harrisburg, Pennsylvania, is an insurance company. Capital Advantage is a wholly-owned subsidiary of Capital BlueCross.

19. Defendant Capital BlueCross, a Pennsylvania non-profit corporation with its principal place of business in Harrisburg, Pennsylvania, is a health insurance company. Capital BlueCross owns Avalon and Dominion National through its wholly-owned subsidiary Capital Advantage Insurance Company. Dominion National provides dental insurance and administers dental benefits on behalf of members of Capital BlueCross.

20. The Dominion Defendants' corporate structure appears as follows:



21. Defendant Providence Health Plan is a health insurance company with its principal place of business in Beaverton, Oregon. Providence Health Plan obtains claim administration services from one or more of the Dominion National Defendants.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000.00 exclusive of interest and costs, there are more than 100 putative Class Members, and minimal diversity exists because many putative Class Members are citizens of a different state

than Defendants. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

23. This Court has personal jurisdiction over the Dominion National defendants (Dominion Dental USA, Dominion Dental Services USA, Dominion Dental Services, Dominion National Insurance Company, and Dominion Dental Services of New Jersey) because they are headquartered in and/or maintain their principal places of business in this District. Dominion National is authorized to and regularly conducts business in Virginia. Dominion National makes decisions regarding corporate governance and management, including decisions regarding the security measures to protect its customers' Personal Information within this District. Dominion National intentionally avails itself of this jurisdiction by promoting, selling and marketing its services from Virginia to consumers across the country.

24. This Court has personal jurisdiction over Avalon because it regularly conducts business in Virginia, including by insuring insurance policies in Virginia and contracting with Virginia entities for the provision of claims administration services. Avalon has sufficient minimum contacts in Virginia such that Avalon intentionally avails itself of this Court's jurisdiction by conducting operations here and promoting, selling and marketing its services to consumers within this District.

25. This Court has personal jurisdiction over Capital Advantage because it regularly conducts business in Virginia, including contracting with entities in Virginia for claims administration services. Capital Advantage has sufficient minimum contacts in Virginia such that Avalon intentionally avails itself of this Court's jurisdiction by conducting operations here and promoting, selling and marketing its services to consumers within this District.

26. This Court has personal jurisdiction over Capital BlueCross because it regularly

conducts business in Virginia, including contracting with Virginia entities for claims administration services. Capital BlueCross has sufficient minimum contacts in Virginia such that Capital BlueCross intentionally avails itself of this Court's jurisdiction by conducting operations here and promoting, selling and marketing its services to consumers within this District.

27. This Court has personal jurisdiction over Providence Health Plan because it has sufficient minimum contacts with Virginia such that Provide Health Plan intentionally avails itself of this Court's jurisdiction, by contracting with Dominion National to provide dental plan administration services in Virginia for its insureds and providing the Personal Information of its insureds to Dominion National in Virginia.

28. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Dominion National's headquarters and principal place of business are located in this District, and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made by Dominion National's governance and management personnel that led to the Data Breach. Moreover, Defendants Capital BlueCross, Capital Advantage, and Avalon conduct business in this District, and market and provide services to consumers within this District.

FACTUAL ALLEGATIONS

A. Defendants Knew They Were Targets of Cyber-Threats

29. Dominion National is a group of related entities that provides dental and vision insurance and administrates dental and vision benefits in the Mid-Atlantic region. These companies are based in Arlington, Virginia. Incorporated in 1996, Dominion National describes itself as "an agile and innovative provider and administrator of dental and vision benefits" that "serves over 875,000 members, including leading health plans, employer groups, municipalities,

associations and individuals among its diverse client base."[4]

30. Dominion National's dental and vision plans are underwritten by Dominion National Insurance Company for members in Georgia and New Jersey, and its vision plans are underwritten by Avalon Insurance Company for members in the District of Columbia, Delaware, Maryland, Pennsylvania, and Virginia. Dominion National also provides dental insurance and administers dental benefits on behalf of members of BlueCross Dental, a dental plan offered by Capital BlueCross based in Harrisburg, Pennsylvania. Dominion Dental Services USA administrates the dental and vision benefits for these plans as well as other third-party insurers. For example, Dominion National also provides dental claims administration for Providence Health Plan, a health insurer based in Oregon.

31. As part of its business operations, Dominion National collects significant amounts of sensitive personal, financial, and medical information. As such, Dominion National acknowledges that it has a duty and obligation to store securely such information and maintains a number of privacy practices and policies governing its responsibilities for doing so.

32. For example, Dominion National maintains a Code of Conduct which applies to its employees, officers, committee members, and directors. Under the heading "Commitment to Protection of Employee and Member Information," the Code of Conduct states: "Dominion is committed to protecting the Protected Health Information (PHI) of its members," and "[a]t Dominion, we are committed to protecting confidential information, including employee and member information. Dominion restricts access to confidential employee-related information only to those employees and vendor/service providers who need the data to provide services to our

[4] DominionNational.com, News, https://www.dominionnational.com/news/2017-02-28 (last visited Nov. 22, 2019).

employee population. Reasonable caution is taken to maintain physical, electronic, and procedural safeguards to protect this personal data. The safeguards are reviewed periodically by both independent and internal auditors."[5]

33. The Code of Conduct acknowledges the significant amount of sensitive information the company collects and its "obligation to diligently protect the privacy and the security of that information":

> Dominion 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 privacy and the security of that information. Most Member information is considered PHI [Protected Health Information], 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. This includes verbal conversations in the hallway or on the telephone, information printed out, and information sent back and forth by email, fax, regular mail, etc. Questions about any privacy issue related to Member information should be directed to the Privacy Office.[6]

34. The policies and commitments set forth in the Code of Conduct are intended to benefit and protect the individuals who provide their Personal Information to Dominion National in exchange for insurance claims administration.

---

[5] Dominion National, 2019 Code of Business Conduct, at 6, https://dominionnational.com/sites/default/files/Misc/2019%20Dominion%20Code%20of%20Conduct.pdf (last visited Nov. 22, 2019).

[6] *Id*. at 11, 12.

35. Avalon[7] and Capital BlueCross[8] maintain Codes of Conduct that make identical representations concerning data security. Indeed, the language quoted above is found in the Avalon and Capital BlueCross Codes of Conduct, with the only material difference being the substitution of the names Avalon and Capital BlueCross, respectively, for Dominion.

36. Dominion National also disseminates a HIPAA-mandated "Notice of Privacy Practices." It provides: "One of our primary goals is to safeguard your PHI [Protected Health Information]. 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 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. In addition, Dominion policy restricts us from sharing your information with employers who sponsor group health plans."[9]

37. Dominion further states in this Notice of Privacy Practices that it is "legally required to follow the privacy practices" described in the notice.[10] Indeed, Dominion expressly acknowledges "Our Legal Duty to Protect the Privacy of Your PHI" which includes information

---

[7] Avalon, 2019 Code of Business Conduct, https://www.avaloninsurance.com/wps/wcm/connect/prod_nws.avaloninsurance.com-2585/8e7ea40d-8ad0-485a-99b3-9976358edd72/av-code-of-conduct.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=ROOTWORKSPACE.Z18_4G00HA41L0J4D0A12EPVOS1000-8e7ea40d-8ad0-485a-99b3-9976358edd72-mLtdiiC (last visited Nov. 22, 2019).

[8] Capital BlueCross, 2019 Code of Business Conduct, https://www.capbluecross.com/wps/wcm/connect/prod_nws.capblue.com29556/8f7d0ad0-f2a5-4611-a719-5928742a7d15/cbc-code-of-conduct.pdf?MOD=AJPERES&CVID=mMFBjZy (last visited Nov. 22, 2019).

[9] Dominion National, Notice of Privacy Practices at 1, https://dominionnational.com/files/Privacy_Policy_Forms/DN_Privacy%20Notice.pdf (last visited Nov. 22, 2019).

[10] *Id.*

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."

38. Likewise, Avalon[11], Capital BlueCross[12], and Providence Health Plan[13] maintain and distribute to their insureds mandated "Notice of Privacy Practices" for their plan members, and Avalon and Dominion maintain a joint policy for members who enroll in both plans.[14]

39. Avalon's and Capital BlueCross's respective Notice of Privacy Practices are virtually identical to the one issued by Dominion, except the name "Avalon Insurance Company" and "Capital BlueCross" are substituted in for Dominion.

40. Dominion National further publishes a "Notice Concerning Financial Information," which commits to protecting dental plan members' financial information. It promises: "An important part of our commitment is our pledge to protect your personal financial information. … We do not disclose your personal financial information, except as permitted by law. We do not disclose this information, even when our customer relationships end, except as permitted by law. … Our policies restrict access of your information to employees who need this information to provide our products and services to you and as permitted by law. We maintain physical,

---

[11] Avalon, Notice of Privacy Practices, https://dominionnational.com/files/Privacy_Policy_Forms/Avalon_Privacy.pdf (last visited Nov. 22, 2019).

[12] Capital BlueCross, Notice of Privacy Practices, https://www.capbluecross.com/wps/wcm/connect/prod_nws.capblue.com29556/5f95004f-6dd9-491e-97fa-fc7deeea0c05/notice-of-privacy-practices.pdf?MOD=AJPERES&CVID=mh1I-L. (last visited Nov. 22, 2019).

[13] Providence Health Plan, Notice of Privacy Practices, https://healthplans.providence.org/about-us/privacy-notices-policies/notice-of-privacy-practices/ (last visited Nov. 22, 2019).

[14] Dominion National and Avalon, Notice of Privacy Practices, https://dominionnational.com/files/Privacy_Policy_Forms/DN_Avalon_Privacy%20Notice.pdf (last visited Nov. 22, 2019).

electronic, and procedural safeguards that comply with legal requirements to protect your personal financial information."[15]

41. Again, Avalon maintains a substantially-similar policy for vision plan members.[16] The only material difference is that Avalon's name is substituted for Dominion in the policy. Avalon and Dominion National issue a joint policy for members who enroll in both plans with identical language.[17]

42. Additionally, Dominion National maintains a "Computer Use and Information Security Policy" which applies to "Dominion Dental USA, Inc. and its directly and indirectly owned subsidiaries d/b/a Dominion National[.]" The 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."[18] This policy provides that: "Information prepared, generated, received, and/or maintained in written or electronic form by Dominion with the expectation of Dominion and/or another party (e.g., member, provider, or employee) that the information will be kept private and will not be disclosed to unauthorized parties."[19]

43. Dominion National's Computer Use and Information Security Policy maintains

---

[15] Dominion National, Notice Concerning Financial Information, https://dominionnational.com/files/Privacy_Policy_Forms/DN_GLB.pdf (last visited Nov. 22, 2019).

[16] Avalon, Notice Concerning Financial Information, https://dominionnational.com/files/Privacy_Policy_Forms/Avalon_GLB.pdf (last visited Nov. 22, 2019).

[17] Dominion National and Avalon, Notice Concerning Financial Information, https://dominionnational.com/files/Privacy_Policy_Forms/DN_Avalon_GLB.pdf (last visited Nov. 22, 2019).

[18] Dominion Dental USA, Inc. and Subsidiaries Computer Use and Information Security Policy at 1, https://dominionnational.com/files/Privacy_Policy_Forms/IT-110%20Computer%20Use%20and%20Information%20Security%20Policy.pdf (last visited Nov. 22, 2019).

[19] *Id.*

guidelines for, among other things:

a. ***Limiting Information Access***: "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."[20]

b. ***Maintaining Computer Security***: "All individuals are … responsible for protecting computer resources from unauthorized access."[21]

c. ***Device and Media Control***: "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."[22]

d. ***Virus and Malicious Software Protection***: "All computing devices must utilize anti-virus and malware software where appropriate. The software must: [i] Be enabled at all times[;] [ii] Scan for viruses and malware on a regular basis, in accordance with corporate guidelines[;] [iii] Have pattern files updated in accordance with corporate guidelines[;] [iv] Have on-access scanning enabled to ensure that any external files are scanned before being introduced into corporate computers."[23]

e. ***E-mail and the Internet***: "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. ... Access to the Internet must pass through a controlled corporately recognized environment."[24]

f. ***Remote Access***: "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."[25]

g. ***Security Awareness***: "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

[20] *Id*. at 3.

[21] *Id*. at 6.

[22] *Id*.

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

[24] *Id*. at 7.

[25] *Id*.

related to securing PHI and other sensitive information."[26]

44. The Computer Use and Information Security Policy also references an internal "Dominion Information Security Strategy" that is maintained for Dominion National's Information Technology ("IT") Department and "HR-0735, Privacy of Member Information," which are not publicly-available.

45. All of these policies make explicit promises to the individuals who provide their Personal Information to Dominion to protect their data and are clearly intended to benefit these individuals: Plaintiffs and Class Members.

46. Providence Health Plan, which contracted with Dominion for dental and vision claims administration services, maintained similar policies, including policies designed to protect member information when it was shared with third parties. In its notice "Confidentiality of Member Information" and its "Notice of Privacy Practices," Providence disclosed that it "may use or disclose your PHI with individuals who perform business functions on our behalf or provide use with services if the information is necessary for such functions or services." Providence then 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."[27]

47. Plaintiffs' and Class Members' Personal Information is valuable and Plaintiffs and Class Members possess recognized property interests in such Personal Information. Plaintiffs and

[26] *Id.*

[27] Providence Health Plan, Confidentiality of Member Information, https://healthplans.providence.org/about-us/privacy-notices-policies/confidentiality-of-member-information/ (last visited Nov. 22, 2019); Providence Health Plan, Notice of Privacy Practices, https://healthplans.providence.org/about-us/privacy-notices-policies/notice-of-privacy-practices/ (last visited Nov. 22, 2019).

Class Members relinquished this information to Defendants subject to the express and implied promises that Defendants would protect their Personal Information.

48. As reflected in these policies, Defendants were at all times fully aware of their legal duty and contractual obligation to protect members' Personal Information and the risks associated with failing to do so. Indeed, Defendants observed frequent public announcements of data breaches affecting insurance and other health-related industries and knew that information of the type collected, maintained, and stored by Dominion National is highly coveted and a frequent target of hackers.

49. 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.

50. 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."[28] In August 2014, the FBI again warned that it has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information

[28] FBI CYBER DIVISION, PRIVATE INDUSTRY NOTIFICATION: HEALTH CARE SYSTEMS AND MEDICAL DEVICES AT RISK FOR INCREASED CYBER INTRUSIONS FOR FINANCIAL GAIN (Apr. 8, 2014), https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf (last visited Nov. 22, 2019).

(PII)."[29] In 2015, Consumer Affairs reported that 81% of major healthcare or insurance companies had a data breach in the previous two years.[30]

51. These were not hypothetical threats. In August 2014, after a cyber-attack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[31]

52. In early 2015, Anthem, Inc., the second-largest health insurer in the United States, suffered a massive data breach exposing the names, addresses, Social Security Numbers, dates of birth, and employment histories of nearly 80 million current and former plan members nationwide.[32]

53. In March 2015, health insurer Premera Blue Cross announced it suffered a data breach that exposed the medical data and financial information of 11 million customers, including claims data, clinical information, banking account numbers, Social Security Numbers, birth dates and other data in an attack that began in May 2014.[33]

---

[29] FBI CYBER DIVISION, FBI LIAISON ALERT SYSTEM #A-000039-TT, https://info.publicintelligence.net/FBI-TargetingHealthcare.pdf (last visited Nov. 22, 2019).

[30] *At least 81% of major healthcare or health insurance companies had a data breach in the past two years*, Consumer Affairs, 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 (last visited Nov. 22, 2019).

[31] J. Finkle, *FBI warns healthcare firms that they are targeted by hackers*, REUTERS (Aug. 20, 2014), http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last visited Nov. 22, 2019).

[32] C. Riley, *Insurance Giant Anthem Hit by Massive Data Breach*, CNN (Feb. 6, 2015), https://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/ (last visited Nov. 22, 2019).

[33] *Premera Blue Cross Says Data Breach Exposed Medical Data*, THE NEW YORK TIMES (March 17, 2015), https://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html (last visited Nov. 22, 2019).

54. Shortly thereafter, New York-based insurer Excellus BlueCross BlueShield announced a breach that exposed the personal information of 10 million of its plan members in an attack dating back to 2013, including names, dates of birth, Social Security numbers, mailing addresses, telephone numbers, member identification numbers, financial account information and claim information.[34]

55. In its 2019 Data Breach Investigations Report, Verizon noted that there were 927 breaches affecting the insurance and financial industries in 2018 alone, with confirmed data disclosure in 207 of the breaches.[35] The report found that 71% of breaches are "financially motivated" meaning the hackers accessed information with the intention to profit from it.

56. According to a report by the HIPAA Journal, "healthcare data breach statistics clearly show there has been an upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published."[36] As reflected in the chart below, many of the largest healthcare breaches over the last decade have involved millions of patient or member records.

[34] *Cyber Breach Hits 10 Million Excellus Healthcare Customers*, USA TODAY (Sept. 10, 2015), https://www.usatoday.com/story/tech/2015/09/10/cyber-breach-hackers-excellus-blue-cross-blue-shield/72018150/ (last visited Nov. 22, 2019).

[35] Verizon, *2019 Data Breach Investigations Report*, available with subscription at: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf (last visited Nov. 22, 2019).

[36] Healthcare Data Breach Statistics, HIPAA JOURNAL, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Nov. 22, 2019).

Largest Healthcare Data Breaches (2009-2018)

Rank	Name of Covered Entity	Year	Covered Entity Type	Individuals Affected	Type of Breach
1	Anthem Inc.	2015	Health Plan	78,800,000	Hacking/IT Incident
2	Premera Blue Cross	2015	Health Plan	11,000,000	Hacking/IT Incident
3	Excellus Health Plan Inc.	2015	Health Plan	10,000,000	Hacking/IT Incident
4	Science Applications International Corporation	2011	Business Associate	4,900,000	Loss
5	University of California, Los Angeles Health	2015	Healthcare Provider	4,500,000	Hacking/IT Incident
6	Community Health Systems Professional Services Corporations	2014	Business Associate	4,500,000	Hacking/IT Incident
7	Advocate Medical Group	2013	Healthcare Provider	4,029,530	Theft
8	Medical Informatics Engineering	2015	Business Associate	3,900,000	Hacking/IT Incident
9	Banner Health	2016	Healthcare Provider	3,620,000	Hacking/IT Incident
10	Newkirk Products, Inc.	2016	Business Associate	3,466,120	Hacking/IT Incident

57. Despite being a holder of Personal Information for millions of individuals nationwide, Defendants failed to prioritize data security by adopting reasonable data resources security measures to prevent and detect unauthorized access to its databases. Defendants had the resources to prevent a breach and made significant expenditures to promote their dental and vision plans, but neglected to invest adequately in data security, despite the growing number of well-publicized data breaches affecting insurance, healthcare, and other related industries.

B. The Data Breach

58. On April 17, 2019, Dominion National received "an internal alert" on its systems and retained cyber-security firm FireEye Mandiant to conduct an investigation.[37]

59. On April 24, 2019, Dominion National "determined that an unauthorized party may have accessed some of its computer servers" and that such access "may have occurred as early as August 25, 2010." According to the company, "Dominion National moved quickly to clean the affected servers. Dominion National has no evidence that any information was in fact accessed, acquired, or misused."[38]

60. On June 21, 2019, Dominion National issued a press release entitled "Dominion National Identifies and Addresses Data Security Incident" stating that:

> Dominion National has undertaken a comprehensive review of the data stored or potentially accessible from those computer servers and has determined that the data may include enrollment and demographic information for current and former members of Dominion National and Avalon vision, as well as individuals affiliated with the organizations Dominion National administers dental and vision benefits for. The servers may have also contained personal information pertaining to plan producers and participating healthcare providers. The information varied by individual, but may include names in combination with addresses, email addresses, dates of birth, Social Security numbers, taxpayer identification numbers, bank account and routing numbers, member ID numbers, group numbers, and subscriber numbers.[39]

61. The release also referred victims to a website created by Dominion National (DominionNationalFacts.com) that included a message from Dominion National's president and provided additional information regarding the breach.

---

[37] Dominion Dental reports data security breach, MARYLAND HEALTH CONNECTION, https://www.marylandhealthconnection.gov/dominion-dental-reports-data-security-breach/ (last visited Nov. 22, 2019).

[38] Dominion National Identifies and Addresses Data Security Incident (June 21, 2019), https://www.prnewswire.com/news-releases/dominion-national-identifies-and-addresses-data-security-incident-300872972.html (last visited Nov. 22, 2019).

[39] *Id.*

62. On that website, Dominion National promised its members and the class that, "Safeguarding the privacy of your personal information is a top priority for us, and we make every effort to protect your information. Despite these efforts, Dominion National experienced a data security incident. We recognize the frustration and concern that this news may cause, and rest assured we are doing everything we can to protect your information moving forward."[40]

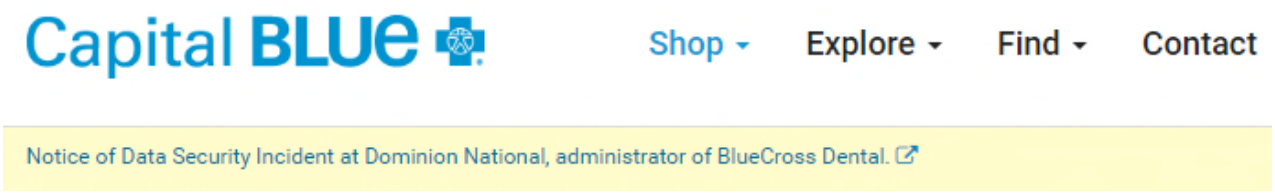
63. The website also provided additional information about what information was accessed: "We have undertaken a comprehensive review of the data stored or potentially accessible from those computer servers and have determined that the data may include enrollment and demographic information for current 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."[41]

64. Both Capital BlueCross and Avalon, on the front pages of their websites, linked to Dominion's website announcing the breach. Capital BlueCross's link stated, "Notice of Data

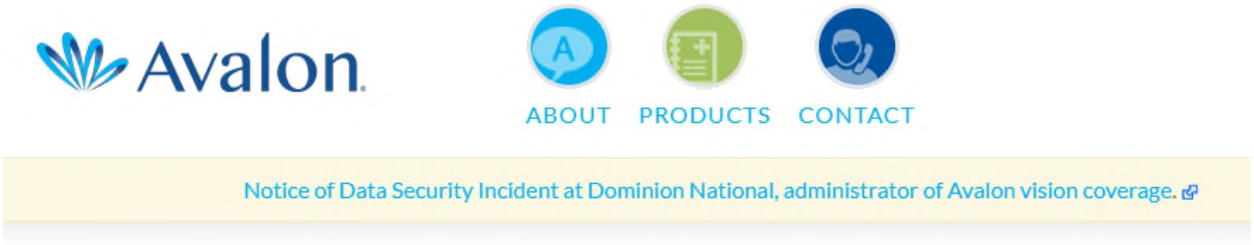
[40] A message from Dominion National President, Mike Davis, https://dominionnationalfacts.com/ (last visited Nov. 22, 2019).

[41] *Id.*

Security Incident at Dominion National, administrator of BlueCross Dental":[42]



65. Similarly Avalon's website announced: "Notice of Data Security Incident at Dominion National, administrator of Avalon vision coverage":[43]



66. 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."[44]

67. Early reports suggest that 2,964,778 individuals were affected in the breach.[45] Dominion National stated that it began mailing notification letters to affected individuals on June 21, 2019.

---

[42] Capital BlueCross, https://www.capbluecross.com/ (as of Aug. 9, 2019).

[43] Avalon, https://www.avaloninsurance.com/ (as of Aug. 9, 2019).

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

[45] 9-Year PHI Breach at Dominion National Impacted 2.9 Million Members, HIPAANSWERS, (July 4, 2019), https://www.hipaanswers.com/9-year-phi-breach-at-dominion-national-impacted-2-9-million-members/ (last visited Nov. 22, 2019).

68. In its notice letter to affected individuals, Dominion National recommended that affected individuals "remain vigilant for incidents of fraud by monitoring your insurance statements and explanation of benefits. If you see services on your insurance statements or explanations of benefits that you did not receive, please call the member/customer services number on your member ID card. We also recommend that you monitor your financial account statements. If you see charges or activity you did not authorize, please contact your financial institution immediately."[46]

69. Dominion National's letter was deficient in providing meaningful notice because it failed to disclose precisely what information was accessed with respect to each affected individual. By failing to identify exactly who was affected or what information was compromised, Dominion National prevented affected individuals from taking meaningful, proactive, and targeted mitigation measures that could help protect them against severe harm.

70. Dominion National also failed to disclose how it was alerted to the breach or explain how the breach went undiscovered for an unprecedented nine years. Experts agree that the extraordinary length of time the breach went undiscovered strongly suggests Dominion National failed to implement reasonable security measures or comply with industry-standard data security practices.

71. For example, Fraser Kyne, Chief Technology Officer at cyber-security firm Bromium, stated in response to the Data Breach: "With highly sensitive data from home addresses, social security numbers and bank details exposed through the breached servers, the length of time this information was open to unauthorized access gives cause for great concern. Nine years is an

[46] *See* Dominion National Sample Data Breach Notice Letter provided to California Attorney General, https://oag.ca.gov/system/files/Dominion%20National%20CA%20Individual%20Notices.pdf (last visited Nov. 22, 2019).

incredibly long time for a hacker to remain undetected with this kind of access. The longer the 'dwell time' (i.e. the time a potential hacker has unauthorized access to systems), the more damage can be caused; hackers will have had ample opportunity to move through systems, potentially insert backdoors, exfiltrate data and spy on communications."[47]

72. Kyne also noted that while it is unclear how the original breach occurred, the most common ways in are emails and browsers, which are accessed through the endpoint. "From there, hackers can make their way through systems to get to their target – in this case the company's servers," Kyne said. "Trying to detect an attack like that in real-time is a fallible approach, and once a hacker has made its way in they can deploy all manner of disguises to stay under the radar. This is why it's important to adopt layered defenses that utilize application isolation to contain malicious threats; preventing hackers from gaining a foothold in the network. That way, if a user does visit an infected site or open a malicious attachment then the malware is rendered harmless; the hacker has nowhere to go, nothing to steal and won't be able to reach company servers."[48]

73. Clyde Hewitt, executive adviser at the security consulting firm CynergisTek, recognized that: "Given the length of time it has taken the company to detect this breach, the number of impacted patients could be extensive. Because the company also appears to be a third-party administrator to self-funded health plans, the number of other impacted covered entities could grow as well."[49]

74. Hewitt also commented that the nine-year breach period "is unusual because it

[47] Alicja Grzadkowska, *Dominion National reveals data breach dating back to 2010*, INSURANCE BUSINESS AMERICA (June 26, 2019), https://www.insurancebusinessmag.com/us/news/cyber/dominion-national-reveals-data-breach-dating-back-to-2010-171071.aspx (last visited Nov. 22, 2019).

[48] *Id.*

[49] Marianne McGee, *Insurer: Breach Undetected for Nine Years*, BANKINFOSECURITY (June 26, 2019), https://www.bankinfosecurity.com/insurer-breach-undetected-for-nine-years-a-12694 (last visited Nov. 22, 2019).

strongly suggests that [Dominion National] may not have been performing comprehensive security audits or performing system activity reviews."[50] Hewitt noted that organizations who report breaches after lengthy delays generally fit into one of two groups: "First, there are organizations that make a conscious decision to underfund their security program to the point that it is incapable of implementing a well-balanced security program being capable of detecting incidents. These organizations may be resource limited or simply haven't translated security into business impacts," said Hewitt. The second group includes organizations with security staff that are "over confident in their own abilities and are unwilling or unable to report the true security posture to senior leadership. This second scenario is common when security responsibilities are assigned to the CIO without having an independent security leader to balance the discussion," he said. "It is also common when individuals are filling security roles without the benefit of appropriate training."[51]

75. Tom Walsh, president of the consultancy tw-Security, stated: "I am surprised that they detected it dating that far back. Most organizations do not retain audit logs or event logs for that long. Most disturbing is that an intruder or a malicious program or code could be into the systems and not previously detected. Nine years is beyond the normal refresh lifecycle for most servers. I would have thought that it could have been detected during an upgrade or a refresh of the hardware."[52]

76. Indeed, the extraordinary length of time the breach went undiscovered strongly suggests that Dominion National: (a) did not regularly update its software or equipment; (b) did not have a sufficient Security Incident & Event Management (SIEM) process in place to identify, monitor, and analyze IT-security events in real time; (c) failed to monitor adequately or log remote

[50] *Id.*

[51] *Id.*

[52] *Id.*

access onto its networks; (d) failed to undertake comprehensive security audits or performing system activity reviews; (e) failed to utilize and run malware and virus detection software; and (f) failed to comply with industry-standard data security measures.

C. Plaintiffs' Individual Allegations

77. Plaintiff Sayed Abubaker was insured by and provided his Personal Information to Avalon in order to obtain vision insurance. Plaintiff Abubaker received a letter from Dominion National dated June 21, 2019 informing him that his Personal Information had been compromised in the Data Breach. As a result of the Data Breach, Plaintiff Abubaker purchased Privacy Guard for $10 per month. He has also expended time and effort monitoring his financial accounts, one account of which has experienced illegal activity over the past year that may have been connected to the Data Breach. Given the highly-sensitive nature of the information stolen, Plaintiff Abubaker remains at a substantial and imminent risk of future harm, including identity theft and medical fraud.

78. Plaintiff Mark Bradley provided his Personal Information to his insurer, Providence Health Plan. Providence Health Plan contracted with Dominion National for the administration of dental benefits starting on January 1, 2015. He received a letter from Dominion National dated August 20, 2019 informing him that his Personal Information had been compromised in the Data Breach. After receiving the notice, Plaintiff Bradley contacted both Providence and Dominion National about the breach; he was told by the Dominion National representative that his social security number and bank routing number had been exposed. Prior to the breach, Plaintiff Bradley had taken care to ensure that his personal information is not exposed to malicious actors. After the breach, Plaintiff Bradley expended time and effort trying to determine the scope of the breach and the exposure of his information. Given the highly-sensitive nature of the information stolen, Plaintiff Bradley, remains at a substantial and imminent future risk of harm, including identity

theft and medical fraud.

79. Plaintiff Joseph Cardiff provided his Personal Information to his insurer, UPMC, to obtain insurance benefits. Plaintiff Cardiff received a letter from Dominion National dated June 21, 2019 informing him that his Personal Information had been compromised in the Data Breach. As a result of the Data Breach, Plaintiff Cardiff purchased Home Title Watch Protection for $200 per year. He has also expended time and effort monitoring his financial accounts in order to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Cardiff remains at a substantial and imminent risk of future harm, including identity theft and medical fraud.

80. Plaintiff Daniel Cho was an in-network provider of dental services for Dominion Dental Services d/b/a Dominion National when he lived in Maryland and supplied his Personal Information to Dominion for that purpose. Cho subsequently moved to Georgia. Plaintiff Cho received a letter from Dominion National dated June 21, 2019 informing him that his Personal Information had been compromised in the Data Breach. As a result of the Data Breach, Plaintiff Cho expended time and effort regularly monitoring his financial accounts and credit score in order to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Cho remains at a substantial and imminent risk of future harm, including identity theft and medical fraud.

81. Plaintiff Magdalyn Hilliard provided her Personal Information to her insurer, Capital BlueCross/BlueCross Dental, in order to obtain dental insurance. Plaintiff Hilliard received a letter from Dominion National dated June 21, 2019 informing her that her Personal Information had been compromised in the Data Breach. As a result of the Data Breach, Plaintiff Hilliard expended time and effort monitoring her credit score in order to mitigate against potential harm,

and Plaintiff Hilliard also contacted the IRS about funds owed, which may have been a result of the Data Breach. She was notified on October 1, 2019 of an account that was opened in her name in Texas. Given the highly-sensitive nature of the information stolen, Plaintiff Hilliard remains at a substantial and imminent risk of future harm, including identity theft and medical fraud.

82. Plaintiff Matthew Slate provided his Personal Information to his insurer, UnitedHealthcare, who in turn supplied his information to Dominion National as its dental benefits administrator. On June 21, 2019, he received a notice letter from Dominion National informing him that his Personal Information had been compromised in the Data Breach. As a result of the Data Breach, Plaintiff Slate spent many hours researching the breach and tracking his credit. Given the highly-sensitive nature of the information stolen, Plaintiff Slate remains at a substantial and imminent risk of future harm, including identity theft and medical fraud.

83. The hackers who breached Dominion National's servers intentionally targeted the personal, financial, and health information of individuals like Plaintiffs.

D. Defendants Had an Obligation to Protect Personal Information Under Federal Law

84. While Dominion National had its systems breached, all Defendants had a non-delegable duty to ensure that all information they collected and stored was secure, and that any entities with whom they shared member information maintained adequate and commercially-reasonable data security practices to ensure the protection of plan members' Personal Information.

85. Defendants are entities covered by HIPAA (*see* 45 C.F.R. § 160.102) and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

86. These rules establish national standards for the protection of patient information,

including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

87. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[53]

88. HIPAA requires that Defendants implement appropriate safeguards for this information.[54]

89. HIPAA requires that Defendants provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons – i.e. non-encrypted data.[55]

90. Despite these requirements, Defendants failed to comply with their duties under HIPAA and their own Privacy Practices. Indeed, Defendants failed to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Protect adequately Plaintiff's and the Class Members' Personal Information;

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to

[53] 45 C.F.R. § 164.502.

[54] 45 C.F.R. § 164.530(c)(1).

[55] 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

91. Defendants failed to comply with their duties under HIPAA and their own Codes of Conduct and Privacy Policies despite each being aware of the risks associated with unauthorized access of members' Personal Information.

E. Defendants Failed to Comply with Regulatory Guidance

92. Federal agencies have issued recommendations and guidelines to temper data breaches and the resulting harm to individuals and financial institutions. For example, the Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance

of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[56]

93. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[57] Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[58]

94. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[59]

95. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable

---

[56] Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Nov. 22, 2019).

[57] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Nov. 22, 2019).

[58] *Id.*

[59] FTC, *Start With Security*, *supra* note 56.

and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[60]

96. In this case, Defendants were fully aware of their obligation to use reasonable measures to protect the personal information of its customers, acknowledging as much in their own privacy policies. Defendants also knew they were targets for hackers. But despite understanding the consequences of inadequate data security, Defendants failed to comply with industry-standard data security requirements or vetting procedures of third-parties with whom they shared their insureds' Personal Information.

97. Defendants failure to employ reasonable and appropriate measures to protect against unauthorized access to members' information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

F. The Effect of the Data Breach on Affected Individuals

98. Given the sensitive nature of the Personal Information stolen in the Data Breach – including names, addresses, email addresses, dates of birth, Social Security numbers, taxpayer identification numbers, member ID numbers, group numbers, subscriber numbers, and bank account and routing numbers – hackers have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future.

99. In fact, many victims of the Data Breach have likely already experienced harms as

[60] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Nov. 22, 2019).

the result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud, unauthorized lines of credit opened in their names, medical and healthcare fraud, and unauthorized access to their bank accounts. Plaintiffs and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, contacting their financial institutions, checking credit reports, and spending time and effort searching for unauthorized activity.

100. The Personal Information exposed in the Data Breach is highly-coveted and valuable on underground or black markets. For example, a cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web" – exposing consumers to identity theft and fraud for years to come. Identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and healthcare-related fraud; (h) access financial accounts and records; or (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest. Medical data is particularly valuable because unlike financial information, such as credit card numbers which can be quickly changed, medical data is static. This is why companies possessing medical information, like Defendants, are intended targets of cyber-criminals.

101. The Personal Information also has substantial legitimate value to Defendants. As Defendants' privacy policies recognize, they use Plaintiffs' Personal Information for business purposes other than administering claims. Many companies that retain Personal Information like

that exposed in the data breach attribute inherent monetary value to it—even listing it as an asset on their books or using it as collateral or consideration for other transactions. Personal Information, including de-identified medical information, is a valuable commodity in the data-driven market place and is often sold and traded between companies—subject to legal and contractual restrictions.

102. And consumers are injured every time their data is stolen and placed on the dark web—even if they have been victims of previous data breaches. Not only is the likelihood of identity theft increased, but the dark web is not like Google or eBay. It is comprised of multiple and discrete repositories of stolen information. Each data breach puts victims at risk of having their information uploaded to different dark web databases, and viewed and used by different criminal actors.

103. Exposure of this information to the wrong people can have serious consequences. The impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[61] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

104. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many

[61] Identity Theft Resource Center, *The Aftermath 2017*, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited Nov. 22, 2019).

> obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[62]

105. The unauthorized disclosure of Social Security Numbers can be particularly damaging because Social Security Numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until damage has been done. Furthermore, as the Social Security Administration warns:

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other Personal Information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other Personal Information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you will not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[63]

---

[62] FTC, *Combating Identity Theft A Strategic Plan* (April 2007), available at https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited Nov. 22, 2019).

[63] Social Security Administration, *Identity Theft and Your Social Security Number* (June 2017), available at http://www.ssa.gov/pubs/10064.html (last visited Nov. 22, 2019).

106. According to the Attorney General of the United States, Social Security numbers "can be an identity thief's most valuable piece of consumer information."[64] Indeed, as explained recently: "The ubiquity of the SSN as an identifier makes it a primary target for both hackers and identity thieves….When data breaches expose SSNs, thieves can use these numbers—usually combined with other pieces of data—to impersonate individuals and apply for loans, housing, utilities, or government benefits. Additionally, this information may be sold on the black market to other hackers."[65]

107. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. purchasing services they would not have otherwise paid for and/or paying more for services than they otherwise would have paid, had they known the truth about Defendants' sub-standard data security practices;

b. losing the inherent value of their Personal Information;

c. losing the value of the explicit and implicit promises of data security;

d. identity theft and fraud resulting from the theft of their Personal Information;

e. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

f. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

g. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

---

[64] *Fact Sheet: The Work of the President's Identity Theft Task Force*, DOJ 06-636, 2006 WL 2679771 (Sep. 19, 2006).

[65] Daniel J. Marcus, *The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information*, 68 Duke L.J. 555, 564–65 (2018).

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

j. the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

108. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[66]

109. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[67]

110. Plaintiffs and Class Members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye Mandiant, approximately 50% of

[66] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Nov. 22, 2019).

[67] U.S. Government Accountability Office Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited Nov. 22, 2019).

consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[68]

111. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, Defendants would have no reason to tout their data security efforts to their actual and potential customers. Further, consumers of health insurance services expect that their insurers and any third parties that are provided with their Personal Information will utilize all necessary measures to protect their data from unauthorized exposure.

112. Consequently, had consumers known the truth about Defendants' data security practices – that they did not adequately protect and store their Personal Information – they would not have purchased health plans from Defendants or would have paid significantly less. As such, Plaintiffs and Class Members did not receive the benefit of their bargain with Defendants because they paid for the value of services they expected but did not receive.

CLASS ACTION ALLEGATIONS

113. Plaintiffs seek relief individually and as representatives of all others who are similarly situated. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3) and/or (c)(4), Plaintiffs seek certification of a nationwide class defined as follows:

> All persons in the United States, its territories, and within sovereign Indian nations whose Personal Information was compromised as a result of the data breach announced by Dominion National on or about June 21, 2019 (the "Class" or

[68] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited Nov. 22, 2019).

"Nationwide Class").

114. Excluded from the Class (and from each of the Subclasses identified below) are Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded are all persons who make a timely election to be excluded from the Class and any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

115. Pursuant to Rule 23, Plaintiffs assert claims under the law of the states of Georgia, Maryland, Oregon, Pennsylvania, Virginia and Washington D.C., on behalf of separate statewide classes, defined as follows:

> All persons in the State of Georgia whose Personal Information was compromised as a result of the data breach announced by Dominion National on or about June 21, 2019 (the "Georgia Subclass").
>
> All persons in the State of Maryland whose Personal Information was compromised as a result of the data breach announced by Dominion National on or about June 21, 2019 (the "Maryland Subclass")
>
> All persons 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 (the "Oregon Subclass")
>
> All persons in the State of Pennsylvania whose Personal Information was compromised as a result of the data breach announced by Dominion National on or about June 21, 2019 (the "Pennsylvania Subclass").
>
> All persons in the State of Virginia whose Personal Information was compromised as a result of the data breach announced by Dominion National on or about June 21, 2019 (the "Virginia Subclass")
>
> All persons in the District of Columbia whose Personal Information was compromised as a result of the data breach announced by Dominion National on or about June 21, 2019 (the "District of Columbia Subclass").

116. Pursuant to Rule 23, Plaintiffs assert claims for the following subclasses of insureds as follows:

> All persons in the United States insured by Providence Health Plan at any time, whose dental plan benefits were administered by Dominion National and whose Personal Information was compromised as a result of the data breach announced by Dominion National on or about June 21, 2019 (the "Providence Health Plan Subclass").
>
> All persons in the United States insured by Avalon Insurance Company at any time, whose Personal Information was compromised as a result of the data breach announced by Dominion National on or about June 21, 2019 (the "Avalon Subclass").
>
> All persons in the United States insured by Capital BlueCross at any time, whose Personal Information was compromised as a result of the data breach announced by Dominion National on or about June 21, 2019 (the "Capital BlueCross Subclass").
>
> All persons in the United States insured by Dominion Dental Services at any time, whose Personal Information was compromised as a result of the data breach announced by Dominion National on or about June 21, 2019 (the "Dominion Dental Services Subclass").

117. Plaintiffs hereby reserve the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery. Plaintiff reserves the right to propose other subclasses prior to trial.

118. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class Members is unknown to Plaintiffs at this time, the proposed Class includes potentially millions of individuals whose Personal Information was compromised in the Data Breach. Class Members may be identified through objective means. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include electronic mail, U.S. mail, internet postings, and/or published notice.

119. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include, but are not limited to:

a. Whether Defendants knew or should have known of the susceptibility of Dominion National's systems to a data breach;

b. Whether Defendants failed to implement reasonable and adequate security procedures and practices;

c. Whether Dominion National's security measures to protect its systems were reasonable in light known legal requirements;

d. Whether Defendants' efforts (or lack thereof) to ensure the security of members' Personal Information provided to Dominion National were reasonable in light of known legal requirements;

e. Whether Defendants owed a duty to Plaintiff and Class Members to protect their Personal Information;

f. Whether Defendants breached their duty to protect the Personal Information of Plaintiff and Class Members by failing to provide adequate data security;

g. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of Dominion National's systems and/or the loss of the Personal Information of Plaintiffs and Class Members;

h. Whether Defendants had a contractual obligation to use reasonable security measures and whether they complied with such contractual obligations;

i. Whether Defendants' conduct amounted to violations of state consumer protection statutes, and/or state data breach statutes;

j. Whether, as a result of Defendants' conduct, Plaintiffs and Class Members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled; and,

k. Whether, as a result of Defendants' conduct, Plaintiffs and Class Members are entitled to injunctive, equitable, declaratory, and/or other relief, and, if so, the nature of such relief.

120. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other Class Members. Plaintiffs' Personal Information was in Defendants' possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to other Class Members and Plaintiffs seek relief consistent with the relief of the Class.

121. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate class representatives because their interests do not conflict with the interests of Class Members who they seek to represent, Plaintiffs have retained counsel competent and experienced in complex class action litigation and data breach litigation, and Plaintiffs intend to prosecute this action vigorously. The Class Members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

122. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and Class Members are relatively small compared to the burden and expense required to individually litigate their claims against Defendants, and thus, individual litigation to redress Defendants' wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential

for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

123. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

124. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Defendants' owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Defendants failed to take reasonable steps to safeguard the Personal Information of Plaintiffs and Class Members;

c. Whether Defendants failed to adequately monitor and audit the data security systems of Dominion National.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class, or alternatively, Plaintiffs and their respective Subclasses, against the Dominion Defendants)

125. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

126. Defendants required Plaintiffs and Class Members to submit Personal Information

to obtain health insurance and claims administration services, and in some instances, shared member data amongst each other in order to administer insurance benefits. Defendants collected and stored the data for commercial gain.

127. Defendants had a non-delegable duty to ensure that the information they collected and stored and that any associated entities with whom they shared patient information maintained adequate and commercially-reasonable data security practices to ensure the protection of members' Personal Information.

128. Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting the Personal Information within their control from being compromised, lost, stolen, accessed and misused by unauthorized persons. Indeed, Defendants acknowledged this duty in its numerous policies in which it promised to protect Plaintiffs' and Class Members' Personal Information.

129. Defendants owed a duty of care to Plaintiffs and Class Members to provide security, consistent with industry standards, to ensure that the systems and networks adequately protected the Personal Information.

130. Defendants owed a duty of care to Plaintiffs and Class Members to adequately vet any third-parties to whom they provided Plaintiffs and Class Members Personal Information, including requesting information about the third-party's data security policies, procedures, protocols and measure and verifying that the third-party's data security was actually sufficient to protect Plaintiff's and Class Member's Personal Information from unauthorized exposure.

131. Defendants' duty to use reasonable care in protecting Personal Information arose as a result of the common law and the statutes and regulations, such as the HIPAA regulations described above, as well as their own policies and promises regarding privacy and data security.

132. Defendants knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities in Dominion National's systems, and the importance of adequate security.

133. Defendants breached their common law, statutory, and other duties – and thus were negligent – by failing to use reasonable measures to protect patients' Personal Information, and by failing to provide timely and adequately detailed notice of the Data Breach.

134. Defendants breached their duties to Plaintiffs and Class Members in numerous ways, as described herein, including by:

a. failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the Personal Information of Plaintiffs and Class Members;

b. failing to comply with industry standard data security standards during the period of the Data Breach;

c. failing to comply with their own policies;

d. failing to comply with regulations protecting the Personal Information at issue during the period of the Data Breach;

e. failing to adequately monitor, evaluate, and ensure the security of Dominion National's network and systems;

f. failing to recognize in a timely manner that the Personal Information of Plaintiffs and Class Members had been compromised;

g. failing to disclose timely and adequately that the Personal Information of Plaintiffs and Class Members had been compromised.

135. Plaintiffs' and Class Members' Personal Information would not have been

compromised but for Defendants' wrongful and negligent breach of their duties.

136. Defendants' failure to take proper security measures to protect sensitive Personal Information of Plaintiffs and Class Members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Personal Information of Plaintiffs and Class Members. Plaintiffs and Class Members are part of a well-defined, foreseeable, finite and discernible group that was at high risk of having their Personal Information misused if disclosed or not protected by Dominion National.

137. It was also foreseeable that Defendants' failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and Class Members.

138. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury and damages described herein, including, but not limited to: ongoing, imminent and 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 publication and/or theft of their Personal Information; the illegal sale of their Personal Information on the deep web black market; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; costs associated with placing freezes on credit reports; decreased credit scores and ratings; lost value of their Personal Information; the continued risk to their Personal Information, which remains in Defendants'

possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Personal Information of current and former members in its continued possession; future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Personal Information for the indefinite future; and other economic and non-economic losses.

SECOND CLAIM FOR RELIEF
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class, or alternatively, Plaintiffs and their respective Subclasses, against the Dominion Defendants)

139. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

140. As a health insurance provider and/or benefits administrator, the Defendants are entities covered by HIPAA, 45 C.F.R. § 160.102. The Defendants are therefore obligated to comply with all rules and regulations under 45 C.F.R. Part 160 and 164.

141. 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."

142. 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.

143. Defendants are 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.

144. 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.

145. Defendants 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.

146. 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.*

147. Defendants breached their notification obligations under HIPAA by failing to give adequate and timely notice of the breach to Plaintiffs and Class Members.

148. HIPAA requires Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health

information" within the meaning of HIPAA.

149. HIPAA further requires Defendants to disclose the unauthorized access and theft of the Personal Information to Plaintiffs and the Class "without unreasonable delay" so that Plaintiffs and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information. *See* 45 C.F.R. § 164.404.

150. Defendants violated HIPAA by failing to reasonably protect Plaintiffs' and Class Members' Personal Information, as described herein.

151. Defendants' violations of HIPAA constitute negligence *per se*.

152. Plaintiffs and Class Members are within the class of persons that HIPAA and its implementing regulations were intended to protect.

153. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

154. Additionally, Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Personal Information. 15 U.S.C. § 45(a)(1).

155. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

156. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Personal Information they obtained, stored, and disseminated in the regular course of their business, and the foreseeable

consequences of a data breach, including, specifically, the significant damage that would result to Plaintiffs and Class Members.

157. Defendants' violations of Section 5 of the FTC Act constitute negligence *per se*.

158. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

159. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

160. As a direct and proximate result of Defendants' negligence *per se* under HIPAA and the FTC Act, Plaintiffs and Class Members have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

THIRD CLAIM FOR RELIEF
VIOLATION OF VIRGINIA CONSUMER PROTECTION ACT,
Va. Code § 59.1-196, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class, or in the alternative, Plaintiffs Hilliard and Slate on behalf of the Virginia Subclass, against Dominion Dental Services USA and Dominion Dental USA)

161. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

162. Defendants, Plaintiffs, and the Class Members are "persons" within the meaning of § 59.1-198 of the Virginia Consumer Protection Act ("VCPA").

163. Defendants are not insurance companies regulated by the Virginia State Corporation Commission or by another comparable federal regulating body.

164. Defendants engaged in deceptive practices in the conduct of its business in violation of the VCPA, § 59.1-200, as described herein, including:

a. Representing that its services have characteristics they do not have;

b. Representing that its services are of a particular standard, quality, grade, style, or model;

c. Advertising services with the intent not to sell them as advertised; and

d. Using deception, fraud, false pretense, false promise, and making material omissions in connection with a consumer transaction.

165. Defendants' deceptive trade practices, as described herein, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Making material omissions about and misrepresenting its ability to protect the privacy and confidentiality of Plaintiff and Class Members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Making material omissions about and misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Personal Information, including duties imposed by HIPAA and

the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Class Members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45.

166. Defendants representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

167. Defendants acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Plaintiff and Class Members' rights. Breaches within the insurance and health industry put Defendant on notice that their security and privacy protections were inadequate.

168. Had Defendants disclosed to Plaintiff and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and Class Members' Personal Information as part of the services Defendant provided and for which Plaintiff and Class Members paid without advising that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class Members' Personal Information. Accordingly, Plaintiff and the Class members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

169. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain made with Defendant through their dental and vision insurers; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

170. Plaintiff and Class members seek all relief allowed by law, including actual damages, alternative statutory damages of $500 or $1000 if Defendants' conduct is found to be willful, and reasonable attorneys' fees and costs, under Va. Code § 59.1-204.

FOURTH CLAIM FOR RELIEF
BREACH OF CONTRACT
(On Behalf of Plaintiffs Hilliard, Abubaker, and Cho and the Capital BlueCross, Avalon, and Dominion Dental Services Subclasses, against Capital BlueCross, Avalon, Dominion Dental Services Inc.)

171. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

172. Plaintiff Hilliard was insured by Capital BlueCross. Plaintiff Abubaker was insured by Avalon. Plaintiff Cho was an in-network provider for Dominion Dental Services Inc.

173. Defendants each disseminated a "Notice of Privacy Practices" ("Notice") which constitute an agreement between Defendants and persons who provided their Personal Information to Defendants, including Plaintiffs and Class Members.

174. Plaintiffs and Class Members formed a contract with Defendants and complied with all obligations under such contract when they provided Personal Information to Defendants subject to the Notices.

175. Defendants' Notices states that they "are legally required to follow the privacy

practices that are described in this notice" including (a) implementing policies and procedures throughout their organization to protect members' Personal Information; (b) training all employees on appropriate uses, disclosures, and protection of PHI; (c) limiting employee system access to only the PHI needed to perform job duties; (d) ensuring secure disposal of confidential information; and (e) using unique user IDs and passwords, etc.

176. Defendants breached their agreements with Plaintiffs and Class Members by failing to protect their Personal Information, including by failing to comply with the promises and obligations set forth in the Notices as described herein.

177. Additionally, Defendants issued to Plaintiffs "Notice Concerning Financial Information" which constitute an agreements between Defendants and Plaintiffs and Class Members.

178. Plaintiffs and Class Members who provided their personal information to Defendants formed a contract with Dominion National when they gave their information subject to the Notice Concerning Financial Information.

179. Defendants' Notices Concerning Financial Information state that they will undertake certain obligations to ensure members' Personal Information is kept safe. Specifically, Defendants "pledge[d] to protect your personal financial information" and stated that they "do not disclose your personal financial information, except as permitted by law" and that they "do not disclose this information, even when our customer relationships end." Defendants further promised that they "maintain physical, electronic, and procedural safeguard that comply with legal requirements to protect your personal financial information."

180. As a direct and proximate result of these breaches, Plaintiffs and Class Members sustained actual losses and damages as described in detail above, including that they did not receive

the benefits of the bargains for which they paid.

FIFTH CLAIM FOR RELIEF
BREACH OF CONTRACT AS THIRD-PARTY BENEFICIARIES
(On Behalf of Plaintiffs and the Nationwide Class, or alternatively, Plaintiffs and their respective State Subclasses, against the Dominion Defendants)

181. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

182. Defendants each maintain a "Code of Conduct" that constitutes an agreement between Defendants and their respective employees, officers, committee members, and directors.

183. The Code of Conduct was entered into for the express benefit of current and former plan members and current and former plan members of insurance plans whose dental and/or vision benefits were administered by Dominion National, including Plaintiffs and Class Members.

184. Plaintiffs and members of the Class are third-party beneficiaries of Defendants' Codes of Conduct.

185. Nothing in Defendants' Codes of Conduct expressly excludes third-party beneficiaries, disclaims the existence or creation of third-party beneficiaries, or defines Plaintiffs and Class Members as not being third-party beneficiaries. The commitment to protect member information can only be interpreted as establishing Plaintiffs and Class Members as third-party beneficiaries of Defendants Code of Conduct policies.

186. Defendants breached their agreements and duties and obligations to Plaintiffs and Class Members by failing to protect their Personal Information, including failing to comply with the promises and obligations set forth in the Codes of Conduct. This included failing to:

a. "[P]rotect[] confidential information, including employee and member information";

b. Undertake "[r]easonable caution … to maintain physical, electronic, and procedural safeguards to protect [members'] personal data";

c. Fulfill their "obligation to diligently protect the privacy and the security of [members'] information";

d. "[E]nsur[e] 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."

187. Additionally, Dominion National's "Computer Use and Information Security Policy" constitutes an agreement between Dominion National and persons who provided their Personal Information to Dominion National.

188. Plaintiffs and Class Members who provided their Personal Information to Dominion National formed a contract with Dominion National when they submitted their information, which is subject to the Computer Use and Information Security Policy.

189. Dominion National's Computer Use and Information Security Policy states that it will undertake certain obligations to ensure members' Personal Information "will be kept private and will not be disclosed to unauthorized parties" including (a) limiting information access; (b) maintaining computer security; (c) implementing device and media control measures to protect Personal Information; (d) implementing virus and malicious software protection; (e) restricting access to Personal Information via electronic mail and the internet; and (f) limiting remote access to Dominion National's computing environment.

190. Dominion National breached its agreement with Plaintiffs and Class Members who provided their Personal Information to Dominion National by failing to protect their Personal Information, including failing to comply with the promises and obligations set forth in the Computer Use and Information Security Policy.

191. As a direct and proximate result of these breaches, Plaintiffs and Class Members sustained actual losses and damages as described in detail above, including that they did not receive

the benefits of the bargains for which they paid.

SIXTH CLAIM FOR RELIEF
BREACH OF CONTRACT AS THIRD PARTY BENEFICIARY
(On Behalf of Plaintiffs and the Nationwide Class, or alternatively, Plaintiffs and their respective State Subclasses, against Dominion Dental Services USA and Dominion Dental USA)

192. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

193. Plaintiffs and Class Members are insured by entities, including but not limited to the Defendants, that contract with Defendant Dominion Dental Services USA, Inc. or Dominion Dental USA, Inc. for administration of dental and vision claims.

194. Defendant Dominion Dental Services USA and Dominion Dental USA entered into contracts with other Defendants and third-party insurance companies to administer dental and vision benefits and provide other administrative services related to the storage and security of Plaintiffs' and Class Members' Personal Information. On information and belief, these contracts clearly and definitely intended to confer a benefit on Plaintiffs and Class Members, including, but not limited to, administration of their policy benefits and the protection of their Personal Information by Dominion Dental Services USA and Dominion Dental USA.

195. Defendant Dominion Dental Services USA and Dominion Dental USA breached these contracts, to which Plaintiffs and Class Members were third-party beneficiaries, by failing to implement and follow adequate data security protocols, measures, policies and procedures necessary to protect Plaintiffs' and Class Members' Personal Information from exposure.

196. Plaintiffs and Class Members are entitled to enforce these contracts as intended third party beneficiaries.

197. As a direct and proximate result of these breaches, Plaintiffs and Class Members who provided their Personal Information to Dominion Dental Services USA and Dominion Dental USA pursuant to agreements between Plaintiffs' and Class Members' insurers and Dominion

Dental Services USA and Dominion Dental USA sustained actual losses and damages as described in detail above, including that they did not receive the benefits these contracts. Plaintiffs and Class Members are entitled to damages stemming from Dominion Dental Services USA's and Dominion Dental USA's breach of these agreements.

SEVENTH CLAIM FOR RELIEF
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class, or alternatively, Plaintiffs and their respective State Subclasses, against the Dominion Defendants)

198. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein, and assert this claim in the alternative to their breach of contract claims to the extent necessary.

199. Plaintiffs and Class Members were required to provide their Personal Information, including names, addresses, Social Security numbers, financial information, and other personal information to some or all Defendants in order to enroll in health plans or have their health plan benefits administered.

200. As part of these transactions, Defendants agreed to safeguard and protect the Personal Information of Plaintiffs and Class Members. Implicit in these transactions between Defendants and Class Members was the obligation that Defendants would use the Personal Information for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

201. Additionally, Defendants implicitly promised to retain this Personal Information only under conditions that kept such information secure and confidential and therefore had a duty to reasonably safeguard and protect the Personal Information of Plaintiffs and Class Members from unauthorized disclosure or access.

202. Plaintiffs and Class Members entered into implied contracts with the reasonable expectation that Defendants' data security practices and policies were reasonable and consistent

with industry standards. Plaintiffs and Class Members believed that Defendants would use part of the monies paid to Defendants under the implied contracts to fund adequate and reasonable data security practices.

203. Plaintiffs and Class Members would not have provided and entrusted their Personal Information to Defendants or would have paid less for Defendants' services in the absence of the implied contract or implied terms between them and Defendants. The safeguarding of the Personal Information of Plaintiffs and Class Members was critical to realize the intent of the parties.

204. Defendants breached their implied contract with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' Personal Information, which was compromised as a result of the Data Breach.

205. Defendants' acts and omissions have materially affected the intended purpose of the implied contracts, which required Plaintiffs and Class Members to provide their Personal Information in exchange for enrollment in health plans and insurance benefits.

206. As a direct and proximate result of Defendants' breaches, Plaintiffs and Class Members sustained actual losses and damages as described in detail above, including that they did not receive the benefits of the bargains for which they paid.

EIGHTH CLAIM FOR RELIEF
BREACH OF COVENANT OF GOOD FAITH AND FAIR DEALING
(On Behalf of Plaintiffs and the Nationwide Class, or alternatively, Plaintiffs and their respective State Subclasses, against the Dominion Defendants)

207. Plaintiffs restate and re-allege the preceding paragraphs as if full set forth herein.

208. Plaintiffs and Class Members had contracts, third party beneficiary status under contracts, or implied contracts with Defendants under which Defendants had an obligation to implement data security to protect the Personal Information furnished to them by Plaintiffs and Class Members.

209. Defendants were required to act in accordance with this implied covenant of good faith and fair dealing when performing under these contracts.

210. Defendants breached the covenant of good faith and fair dealing by failing to reasonably safeguard Plaintiffs' and Class Members' Personal Information and by failing to implement adequately the data security necessary to protect Personal Information.

211. Plaintiffs and Class Members were injured as a direct result of Defendants' breach of the implied covenant of good faith and fair dealing and sustained actual damages as described in detail above.

NINTH CLAIM FOR RELIEF
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class, or alternatively, Plaintiffs and their respective State Subclasses, against the Dominion Defendants)

212. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein, and assert this claim in the alternative to their breach of contract claims to the extent necessary.

213. Plaintiffs and Class Members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by the Defendants and which was ultimately stolen in the Data Breach. This information is independently valuable.

214. Plaintiffs and Class Members conferred a monetary benefit on Defendants in the form of their personal information or the premiums paid for the purchase of health insurance and health benefits services, including those paid indirectly by Plaintiffs to the Defendants responsible for administering the insurance benefits.

215. Defendants appreciated and had knowledge of the benefits conferred upon them by Plaintiffs and Class Members in the form of their valuable Personal Information and health insurance premiums.

216. The premiums for health insurance and health benefits services that Plaintiffs and Class Members paid (directly or indirectly) to Defendants should have been used by Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

217. Likewise, in exchange for receiving Plaintiffs' and Class Members' valuable Personal Information, which Defendants were able to use for business purposes and which provided actual value to Defendants, Defendants were obligated to devote sufficient resources to reasonable data privacy and security practices and procedures.

218. As a result of Defendants' conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between health insurance and health benefit services with the reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and the inadequate health insurance and health benefits services without reasonable data privacy and security practices and procedures that they received.

219. Under principals of equity and good conscience, Defendants should not be permitted to retain the money Defendants should have and were required to devote to the implementation of adequate data privacy and security practices and procedures that Plaintiffs and Class Members paid for or provided their Personal Information to Defendants in exchange for, and that were otherwise mandated by HIPAA regulations, federal, state and local laws, and industry standards.

220. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds they received from Plaintiffs and Class Members as well as all funds that should have been used for data security in exchange for the receipt of Plaintiffs' and Class Members' valuable Personal Information.

221. Equity and good conscience require restitution by the Defendants in the amount of the benefit conferred on Defendants as a result of their wrongful conduct, including, specifically, the value to Defendants of the Personal Information that was stolen in the Defendants' Data Breach the resulting profits Defendants received and are receiving from the use of that information, and the monies Defendants avoided paying for adequate data security. Further, Defendants should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendants' services.

TENTH CLAIM FOR RELIEF
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Nationwide Class, or Plaintiffs and their respective Subclasses, against the Dominion Defendants)

222. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

223. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the state and federal statutes described in this Complaint.

224. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Personal Information. Plaintiffs allege that Defendants' data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Personal Information and remain at imminent risk that further compromises of their Personal Information will occur in the future.

225. Defendants still possess Personal Information pertaining to Plaintiffs and Class

Members, which means the Personal Information remains at risk of further breaches.

226. Accordingly, Defendants have not satisfied their contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Defendants' lax approach towards data security has become public, Class Members' Personal Information is more vulnerable than it was prior to announcement of the Data Breach.

227. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide data security measures to Plaintiffs and Class Members.

228. Pursuant to the Declaratory Judgment Act, Plaintiffs seek a declaration that (a) Defendants' existing data security measures do not comply with their contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Modifying their practices and policies to ensure they and any business associates to which they provide members' Personal Information engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on their systems on a periodic basis, and ordering vendors to promptly correct any problems or issues detected by such third-party security auditors;

b. Modifying their practices and policies to ensure they and any business associates to which they provide members' Personal Information engage third-party security auditors and internal personnel to run automated security monitoring;

c. Modifying their practices and policies to ensure they and any business associates

to which they provide members' Personal Information audit, test, and train security personnel regarding any new or modified procedures;

d. Modifying their practices and policies to ensure they and any business associates to which they provide members' Personal Information segment Personal Information by, among other things, creating firewalls and access controls so that if one area of a system is compromised, hackers cannot gain access to other portions of the systems;

e. Modifying their practices and policies to ensure Personal Information not necessary for the provision of services is purged, deleted, and destroyed, and to ensure its business associates likewise purge, delete, and destroy such Personal Information;

f. Conducting regular data security audits of any business associates to which they provide members' Personal Information;

g. Routinely and continually conduct internal training and education to inform internal security personnel how to monitor data security or the data security of business associates to whom patients' Personal Information is provided; and

h. Educating their members about the threats they face as a result of the loss of the financial and personal information to third parties, as well as the steps affected individuals must take to protect themselves.

ELEVENTH CLAIM FOR RELIEF
VIOLATION OF MARYLAND CONSUMER PROTECTION ACT,
Md. Code, Comm. Law § 13-101, *et seq.*
(On Behalf of Plaintiff Cho and the Maryland Subclass against Dominion Dental Services USA)

229. Plaintiff Daniel Cho ("Plaintiffs," for purposes of this Count), individually and on behalf of the Maryland Subclass restates and re-alleges the preceding paragraphs as if fully set forth herein.

230. Defendant, Plaintiffs, and the Class Members are "persons" within the meaning of § 13-101(h) of the Maryland Consumer Protection Act ("MCPA").

231. Defendant is not an insurance company authorized to do business in Maryland and is not listed as a regulated entity by the Maryland Insurance Administration.

232. Defendant engaged in deceptive practices in the conduct of its business in violation of the MCPA, § 13-301, as alleged herein, including:

a. Making false and misleading oral and written statements that had the capacity, tendency, or effect of deceiving or misleading consumers;

b. Representing that its services have characteristics they do not have;

c. Representing that its services are of a particular standard, quality, grade, style, or model, which they are not;

d. Failing to state material facts that deceived or tends to deceive consumers;

e. Advertising services with the intent not to sell them as advertised; and

f. Using deception, fraud, false pretense, false promise, and making material omissions in connection with a consumer transaction.

233. Defendant's deceptive trade practices, as alleged herein, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Maryland Subclass Members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maryland Subclass Members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Making material omissions about and misrepresenting its ability to protect the privacy and confidentiality of Plaintiff and Maryland Subclass Members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Making material omissions about and misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maryland Subclass Members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maryland Subclass Members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maryland Subclass Members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45.

234. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Personal Information.

235. Defendant acted intentionally, knowingly, and maliciously to violate Maryland's

Consumer Protection Act, and recklessly disregarded Plaintiff and Maryland Subclass Members' rights. Breaches within the insurance and health industry put Defendant on notice that their security and privacy protections were inadequate.

236. Had Defendant disclosed to Plaintiff and Maryland Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiff's and Maryland Subclass Members' Personal Information as part of the services Defendant provided and for which Plaintiff and Maryland Subclass Members paid without advising that Defendant's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Maryland Subclass Members' Personal Information. Accordingly, Plaintiff and the Maryland Subclass members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

237. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain made with Defendant through their dental and vision insurers; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

238. Plaintiff and Maryland Subclass members seek all relief allowed by law, including actual damages, and reasonable attorneys' fees and costs, under Md. Code § 13-408.

TWELFH CLAIM FOR RELIEF
VIOLATION OF GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT, Ga. Code Ann. §§ 10-1-370, *et seq*.
(On Behalf of Plaintiff Daniel Cho and the Georgia Subclass against Dominion Dental USA and Dominion Dental Services USA)

239. Plaintiff Daniel Cho ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass restates and re-alleges the preceding paragraphs as if fully set forth herein.

240. Defendants, Plaintiff, and Georgia Subclass Members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

241. Defendants Dominion Dental Services USA and Dominion Dental USA are not entities regulated by the Georgia Department of Insurance.

242. Defendants engaged in deceptive trade practices in the conduct of its business, in violation of Ga. Code § 110-1-372(a), as described herein, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised;

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

243. Defendants' deceptive trade practices, as described herein, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Georgia Subclass Members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass Members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Making material omissions and misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Georgia Subclass Members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Making material omissions and misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass Members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Georgia Subclass Members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass Members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45.

244. Defendants' representations and omissions were material because they were likely

to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

245. Defendants intended to mislead Plaintiff and Georgia Subclass Members and induce them to rely on its misrepresentations and omissions.

246. Defendants acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Georgia Subclass Members' rights. Breaches within the insurance and health industry put Defendants on notice that their security and privacy protections were inadequate.

247. Had Defendants disclosed to Plaintiff and Georgia Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and Georgia Subclass Members' Personal Information as part of the services Defendants provided and for which Plaintiff and Georgia Subclass Members paid without advising that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Georgia Subclass Members' Personal Information. Accordingly, Plaintiff and the Georgia Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

248. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff and Georgia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged

herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

249. Plaintiff and Georgia Subclass members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under Ga. Code § 10-1-373.

THIRTEENTH CLAIM FOR RELIEF
VIOLATION OF OREGON UNLAWFUL TRADE PRACTICES ACT,
Or. Stat. §646.605, *et seq.*
(On Behalf of Plaintiff Mark Bradley and the Oregon Subclass against Dominion Dental USA and Dominion Dental Services USA)

250. Plaintiff Mark Bradley ("Plaintiff," for purposes of this Count), individually and on behalf of the Oregon Subclass restates and re-alleges the preceding paragraphs as if fully set forth herein.

251. Defendants, Plaintiff, and Oregon Subclass Members are "persons" within the meaning of § 646.605(4) of the Oregon Unlawful Trade Practices Act ("OUTPA"),

252. Defendants Dominion Dental Services USA and Dominion Dental USA provide administrative services to insurance companies, but do not provide insurance.

253. Defendants engaged in deceptive trade practices in the conduct of its business, in violation of Or. Stat. § 646.608, as described herein, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised;

d. Engaging in other conduct that creates a likelihood of confusion or

misunderstanding.

254. Defendants' deceptive trade practices, as described herein, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Oregon Subclass Members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass Members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Making material omissions and misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Oregon Subclass Members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Making material omissions and misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass Members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Oregon Subclass Members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass Members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45.

255. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

256. Defendants intended to mislead Plaintiff and Oregon Subclass Members and induce them to rely on its misrepresentations and omissions.

257. Defendants acted intentionally, knowingly, and maliciously to violate OUTPA, and recklessly disregarded Plaintiff and Oregon Subclass Members' rights. Breaches within the insurance and health industry put Defendants on notice that their security and privacy protections were inadequate.

258. Had Defendants disclosed to Plaintiff and Oregon Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and Oregon Subclass Members' Personal Information as part of the services Defendants provided and for which Plaintiff and Oregon Subclass Members paid without advising that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Oregon Subclass Members' Personal Information. Accordingly, Plaintiff and the Oregon Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

259. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff and Oregon Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

260. Plaintiff and Oregon Subclass members seek all relief allowed by law, including actual damages, or alternative statutory damages of $200, injunctive relief, and reasonable attorneys' fees and costs under Or. Stat. § 646.641.

FOURTEENTH CLAIM FOR RELIEF
VIOLATION OF PENNSYLVANIA UNFAIR TRADE PRACTICES & CONSUMER PROTECTION LAW, 73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq*.
(On Behalf of Plaintiffs Joseph Cardiff and Magdalyne Hilliard and the Pennsylvania Subclass against Dominion Dental USA, Dominion Dental Services USA, Dominion Dental Services, Avalon, Capital Advantage Insurance Company, and Capital BlueCross)

261. Plaintiffs Joseph Cardiff and Magdalyne Hilliard ("Plaintiff," for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, restate and re-allege the preceding paragraphs as if fully set forth herein.

262. Defendants are "persons", as meant by 73 Pa. Cons. Stat. § 201-2(2).

263. Plaintiff and Pennsylvania Subclass Members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

264. Defendants engaged in unfair methods of competition and unfair or deceptive acts

or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. § 201-3, as described herein, including the following:

a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201-2(4)(vii)); and

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

265. Defendants unfair or deceptive acts and practices, as described herein, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Pennsylvania Subclass Members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass Members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45;

d. Making material omissions and misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Pennsylvania Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Making material omissions and misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Pennsylvania Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45.

266. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

267. Defendants intended to mislead Plaintiff and Pennsylvania Subclass members and induce them to rely on its misrepresentations and omissions.

268. Had Defendants disclosed to Plaintiff and Pennsylvania Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and Pennsylvania Subclass Members' Personal Information as part of the services Defendants provided and for which Plaintiff and Pennsylvania Subclass Members paid without advising that Defendants' data security practices were insufficient to maintain the safety and confidentiality of

Plaintiff's and Pennsylvania Subclass Members' Personal Information. Accordingly, Plaintiff and the Pennsylvania Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

269. Defendants acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Pennsylvania Subclass Members' rights. Data breaches within the insurance and health industry put Defendants on notice that their security and privacy protections were inadequate.

270. As a direct and proximate result of Defendants' unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and the Pennsylvania Subclass Members' reliance on them, Plaintiff and Pennsylvania Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

271. Plaintiff and Pennsylvania Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, restitution, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

FIFTEENTH CLAIM FOR RELIEF
VIOLATION OF DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT,
D.C. Code §§ 28-3904, *et seq*.
(On Behalf of Plaintiff Sayed Abubaker and the District of Columbia Subclass against Dominion Dental USA, Dominion Dental Services USA, Dominion Dental Services, and Avalon)

272. Plaintiff Abubaker ("Plaintiff," for purposes of this Count), individually and on behalf of the District of Columbia Subclass, restates and re-alleges the preceding paragraphs as if fully set forth herein.

273. Defendants are "persons" as defined by D.C. Code § 28-3901(a)(1).

274. Defendants are "merchants" as defined by D.C. Code § 28-3901(a)(3).

275. Plaintiff and District of Columbia Subclass Members are "consumers" who purchased or received goods or services for personal, household, or family purposes, as defined by D.C. Code § 28-3901.

276. Defendants advertised, offered, or sold goods or services in the District of Columbia and engaged in trade or commerce directly or indirectly affecting the people of the District of Columbia.

277. Defendants engaged in unfair, unlawful, and deceptive trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of D.C. Code § 28-3904, as described herein, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, grade, style, or model, when they are of another;

c. Misrepresenting a material fact that has a tendency to mislead;

d. Failing to state a material fact where the failure is misleading;

e. Advertising or offering goods or services without the intent to sell them as advertised or offered;

f. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

278. Defendants' unfair, unlawful, and deceptive trade practices, as described herein, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and District of Columbia Subclass Members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and District of Columbia Subclass Members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Making material omissions and misrepresenting that it would protect the privacy and confidentiality of Plaintiff and District of Columbia Subclass Members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Making material omissions and misrepresenting that it would comply with common

law and statutory duties pertaining to the security and privacy of Plaintiff and District of Columbia Subclass Members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and District of Columbia Subclass Members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and District of Columbia Subclass Members' Personal Information, including duties imposed by HIPAA and the FTC Act, 15 U.S.C. § 45.

279. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

280. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and District of Columbia Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

281. Defendants acted intentionally, knowingly, and maliciously to violate the District of Columbia's Consumer Protection Procedures Act, and recklessly disregarded Plaintiff and District of Columbia Subclass Members' rights. Past data breaches within the insurance and health industry put them on notice that its security and privacy protections were inadequate.

282. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive trade practices, Plaintiff and District of Columbia Subclass Members have suffered and will

continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

283. Plaintiff and District of Columbia Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, injunctive relief, punitive damages, attorneys' fees and costs, the greater of treble damages or $1500 per violation, and any other relief that the Court deems proper.

SIXTEENTH CLAIM FOR RELIEF
BREACH OF CONTRACT
(On behalf of Plaintiff Mark Bradley and the Providence Health Plan Subclass against Defendant Providence Health Plan)

284. Plaintiff Mark Bradley ("Plaintiff," for purposes of this Count), individually and on behalf of the Providence Health Plan Subclass, restates and re-alleges the preceding paragraphs as if fully set forth herein.

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

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

287. 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."

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

289. 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.

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

291. 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.

SEVENTEENTH CLAIM FOR RELIEF
NEGLIGENCE
(On behalf of Plaintiff Mark Bradley and the Providence Health Plan Subclass against Defendant Providence Health Plan)

292. Plaintiff Mark Bradley ("Plaintiff," for purposes of this Count), individually and on behalf of the Providence Health Plan Subclass, restates and re-alleges the preceding paragraphs as if fully set forth herein.

293. 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.

294. 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.

295. 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.

296. 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.

297. 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.

298. 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.

299. 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 Personal Information misused if disclosed or not protected by the companies Providence Health Plan shared it with.

300. 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.

301. Further, Providence was obligated under HIPAA and the FTC Act to protect Plaintiff's and the Providence Health Plan Subclass members' data – obligations which Providence violated by failing to reasonably protect their data as described herein. Providence's violations constitute negligence *per se*.

302. As a direct and proximate result of Providence's conduct, Plaintiff and the Providence Health Plan Subclass members have suffered actual damages, as described herein, and are entitled to monetary relief in an amount to be proven at trial.

REQUEST FOR RELIEF

Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully request that the Court enter judgment in their favor and against Defendants, as follows:

1. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, declare that Plaintiffs are proper class representatives, and appoint Plaintiffs' counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit and prevent Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

3. That the Court award Plaintiffs and Class and Subclass Members compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined at trial;

4. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

5. That the Court order disgorgement and restitution of all earnings, profits,

compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

6. That Plaintiffs be granted the declaratory and injunctive relief sought herein;

7. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

8. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

Dated: November 22, 2019

Respectfully submitted,

By: */s/ Bernard J. DiMuro*

Bernard J. DiMuro (VSB No. 18784)
DIMURO GINSBERG, P.C.
1101 King Street, Suite 610
Alexandria, Virginia 23314
Tel.: (703) 684-4333
bdimuro@dimuro.cosm

Plaintiffs' Liaison Counsel

Kim D. Stephens (*pro hac vice*)
TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
Tel.: (206) 682-5600
kstephens@tousley.com

Barrett J. Vahle (*pro hac vice*)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel.: (816) 714-7100
vahle@stuevesiegel.com

Plaintiffs' Co-Lead and Interim Class Counsel

Swathi Bojedla (*pro hac vice*)
HAUSFELD LLP
1700 K Street NW, Suite 650
Washington, DC 20006
Tel.: (202) 540-7200
sbojedla@hausfeld.com

Thiago M. Coelho (*pro hac vice*)
WILSHIRE LAW FIRM
3055 Wilshire Blvd., 12th Floor
Los Angeles, California 90010
Tel.: (213) 381-9988
thiago@wilshirelawfirm.com

Andrew N. Friedman (*pro hac vice*)
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue, NW, Suite 500
Washington, DC 20005
Tel.: (202) 408-4600
afriedman@cohenmilstein.com

Mark S. Goldman (*pro hac vice*)
GOLDMAN, SCARLATO & PENNY P.C.
8 Tower Bridge, Suite 1025
161 Washington Street
Conshohocken, Pennsylvania 19428
Tel.: (484) 342-0700
goldman@lawgsp.com

Matthew D. Schultz (*pro hac vice*)
LEVIN PAPANTONIO THOMAS MITCHELL RAFFERTY & PROCTOR, P.A.
316 S. Baylen St., Suite 600
Pensacola, Florida 32502
Tel.: (850) 435-7000
mschultz@levinlaw.com

Plaintiffs' Steering Committee