IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. 1:25-cv-1358-DDD-SJP

JULIAN JENKINS,
LYDIA PERRYMAN,
BRENDA PEARSON,
G.I.,
ANTHONY NATOLI, and
GREGORY LEAFE, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

DAVITA, INC.,

Defendant.

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT
AND DEMAND FOR JURY TRIAL

NATURE OF THE ACTION

1. Plaintiffs bring this consolidated amended class action lawsuit on behalf of all persons who entrusted defendant DaVita, Inc. ("DaVita") with highly sensitive Personally Identifiable Information ("PII") and Protected Health Information ("PHI") (collectively "Private Information") that was impacted in a data breach that Defendant publicly disclosed in April 2025 (the "Data Breach" or the "Breach").

2. Plaintiffs' claims arise from DaVita's failure to properly secure and safeguard the Private Information that was entrusted to it, and its accompanying responsibility to store and transfer that information while preserving its confidentiality.

3. DaVita is a leading provider of kidney care services in the United States, offering dialysis and related services to patients with chronic kidney failure and end-stage renal disease through a network of outpatient centers.[1] DaVita delivers care to more than 1.7 million patients.[2]

4. On April 12, 2025, DaVita became aware of a ransomware incident that encrypted certain elements of its IT Network.[3] The Data Breach caused disruptions to DaVita's operations, resulting in DaVita's employees being unable to access DaVita's computer systems.[4] Upon discovery, DaVita launched an investigation to determine the nature and scope of the Data Breach.[5]

5. Upon information and belief, Interlock, a ransomware group, accessed DaVita's IT Network and stole 20+ terabytes of data containing highly sensitive Private Information of DaVita's patients.[6] Interlock attempted ransom negotiations with DaVita but when the negotiations failed, Interlock published Plaintiffs and Class Members Private Information on the dark web.[7]

6. DaVita has since confirmed that it is aware of the ransomware group's claims, and that Private Information was in fact published on the dark web by Interlock.[8]

---

[1] *About*, DaVita, Inc. https://www.davita.com/about (last visited July 28, 2025).

[2] https://investors.davita.com/2018-09-05-DaVita-Medical-Group-Honored-for-Delivering-Excellent-Patient-Care (last visited July 28, 2025).

[3] *Form 8-K*, DaVita Inc., United States Securities and Exchange Commission: https://www.sec.gov/Archives/edgar/data/927066/000119312525079593/d948299d8k.html (last visited July 28, 2025).

[4] *Id.*

[5] *Id.*

[6] *Pietje Kobus*, Kidney Dialysis Provider DaVita Hit by Ransomware Attack (April 14, 2025) https://www.hcinnovationgroup.com/cybersecurity/data-breaches/news/55282892/kidney-dialysis-provider-davita-hit-by-ransomware-attack (last visited July 28, 2025).

[7] *Id.*

[8] https://therecord.media/dialysis-davita-reviewing-data-leak (last visited July 28, 2025).

7. In response to the publication of patients' Private Information, DaVita launched a comprehensive review of the data to identify the exact types of Private Information compromised as well as identify patients affected by the Data Breach.[9]

8. The Data Breach was a direct result of DaVita's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which it was entrusted for treatment with DaVita.

9. Businesses like DaVita's, which collect patients' Private Information, owe individuals to whom the information relates a duty to protect the Private Information from disclosure and theft and to keep it safe and confidential. This duty arises under contract, statutory, and common law, industry standards, representations made to Plaintiffs and Class Members, and because it is foreseeable that hackers with nefarious intentions will target the Private Information and use it to harm the affected individuals.

10. Upon information and belief, DaVita breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiffs and Class Members of DaVita's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize

[9] *The HIPAA Journal*, Ransomware Group Claims Responsibility for DaVita Ransomware Attack; Leaks Data: https://www.hipaajournal.com/davita-ransomware-attack/#:~:text=DaVita%20has%20confirmed%20it%20is,notified%20as%20soon%20as%20possible. (last visited July 28, 2025).

widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

11. DaVita understood its obligations and promised to safeguard Plaintiffs and Class Members' Private Information. Plaintiffs and Class Members relied on these implied promises when seeking out and obtaining DaVita's services. But for this mutual understanding, Plaintiffs and Class Members would not have provided DaVita with their Private Information. DaVita, however, did not meet these reasonable expectations, causing Plaintiffs and Class Members to suffer injury.

12. DaVita disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiffs and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members with prompt and full notice of the Data Breach.

13. In addition, DaVita failed to adequately protect Plaintiffs and Class Members' Private Information by failing to implement industry standard data security procedures, practices, and protocols to protect Plaintiffs and Class Members Private Information from hackers.

14. Prior to the Data Breach Incident, DaVita should have ensured that it had adequate monitoring software in place to detect intrusions or the transfer of large volumes of data to third party networks, that it implemented multi-factor authentication to verify the credentials of individuals attempting to access Private Information, that it limited access to Private Information

to only necessary employees, that it encrypted or tokenized Private Information in internet accessible locations, and that it deleted or redacted Private Information that it was no longer required to maintain. By failing to implement these reasonable and industry standard data security measures, DaVita left Plaintiffs' and Class members' Private Information in a condition vulnerable to unauthorized access.

15. Plaintiffs and Class Members' identities are now at risk because of DaVita's negligent conduct since the Private Information that DaVita collected and maintained is now in the hands of data thieves.

16. As a result of the Data Breach, Plaintiffs and Class Members are now at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiffs and Class Members must now and for years into the future closely monitor their medical and financial accounts to guard against identity theft. As a result of DaVita's unreasonable and inadequate data security practices, Plaintiffs and Class Members have suffered numerous actual and concrete injuries and damages.

17. Plaintiffs and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiffs and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will continue to include in the future, among other things: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

18. Plaintiffs and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity

incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) deprivation of value of their Private Information; and (f) the continued risk to their sensitive Private Information, which remains in the possession of DaVita, and which is subject to further breaches, so long as DaVita fails to undertake appropriate and adequate measures to protect it collected and maintained.

19. Through this amended class action complaint, Plaintiffs seek to remedy these harms on behalf of themselves, and all similarly situated individuals whose Private Information was accessed during the Data Breach.

20. Accordingly, Plaintiffs bring this action against DaVita seeking redress for its unlawful conduct.

21. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to DaVita's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by DaVita, and declaratory relief.

22. The exposure of one's Private Information to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiffs and the Class's Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and unsecure.

PARTIES

23. Plaintiff Julian Jenkins is a natural person and a citizen of South Carolina, where he intends to remain.

24. Plaintiff Lydia Perryman is a natural person and a citizen of Arizona, where she intends to remain.

25. Plaintiff Brenda Pearson is a natural person and a citizen of North Carolina, where she intends to remain.

26. Plaintiff G.I. is a natural person and a citizen of Missouri, where he intends to remain.

27. Plaintiff Anthony Natoli is a natural person and a citizen of California, where he intends to remain.

28. Plaintiff Gregory Leafe is a natural person and citizen of California, where he intends to remain.

29. Defendant DaVita, Inc., is a Delaware corporation, with its principal place of business located at 2000 16th Street, Denver, Colorado, 80202.

JURISDICTION AND VENUE

30. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this Class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than DaVita's state of citizenship.

31. This Court has personal jurisdiction over the parties in this case. DaVita conducts business in this District and is a citizen of this District by virtue of having its principal place of business located in this District.

32. Venue is proper in this District under 28 U.S.C. §1391(b) because DaVita maintains its headquarters in this District and regularly conducts business in this District.

FACTUAL ALLEGATIONS

A. Background on DaVita

33. DaVita is a comprehensive kidney care provider that serves approximately 1.7 million patients[10] at 3,166 outpatient dialysis centers, of which 2,657 centers are located in the United States, and 509 centers are in 13 other countries worldwide.[11]

34. In the ordinary course of receiving DaVita's medical care, services and products, each patient must provide (and Plaintiffs and Class Members did provide) DaVita with sensitive Private Information including: (i) name, (ii) phone number, (iii) email address, (iv) date of birth, (v) Social Security number, (vi) driver's license number and/or state identification card, (vii) payment and financial account information, (viii) health insurance and medical information.

35. DaVita also creates and stores medical records and other protected health information for its patients, records of treatments and diagnoses.

36. DaVita made promises and representations to individuals, including Plaintiffs and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.[12]

37. DaVita agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiffs and Class members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA").

---

[10] https://investors.davita.com/2018-09-05-DaVita-Medical-Group-Honored-for-Delivering-Excellent-Patient-Care (last visited July 28, 2025).

[11] *Id.*

[12] *Privacy Policy*, Davita, Inc., https://www.davita.com/privacy-policy (last visited July 28, 2025).

38. Yet, through its failure to properly secure Plaintiffs and Class Members' Private Information, DaVita failed to meet its own promises and duties to Plaintiffs and Class Members.

B. The Data Breach

39. On April 12, 2025, DaVita became aware of a ransomware attack that encrypted certain elements of its IT Network.[13] The cyber-attack disrupted DaVita's operations, preventing employees access to DaVita's IT Network.[14][15]

40. Upon discovery, DaVita launched an investigation to determine the nature and scope of the Data Breach.[16] Thereafter, DaVita issued a public disclosure of the Data Breach on April 14, 2025, by filing an 8-K report with the U.S. Securities Exchange Commission ("SEC").[17]

41. Shortly after DaVita became aware of the Data Breach, the ransomware group Interlock claimed responsibility, indicating it obtained 20+ terabytes of data from DaVita's IT Network, including Private Information of millions of DaVita's patients.[18]

42. Interlock has rapidly gained notoriety for its high-impact ransomware campaigns in recent years, employing a double-extortion model: encrypting victims' systems and exfiltrating

---

[13] *Form 8-K*, DaVita Inc., United States Securities and Exchange Commission: https://www.sec.gov/Archives/edgar/data/927066/000119312525079593/d948299d8k.html (last visited July 28, 2025).

[14] *Id.*

[15] https://www.reuters.com/technology/cybersecurity/dialysis-firm-davita-hit-by-ransomware-attack-2025-04-14/ (last visited July 28, 2025).

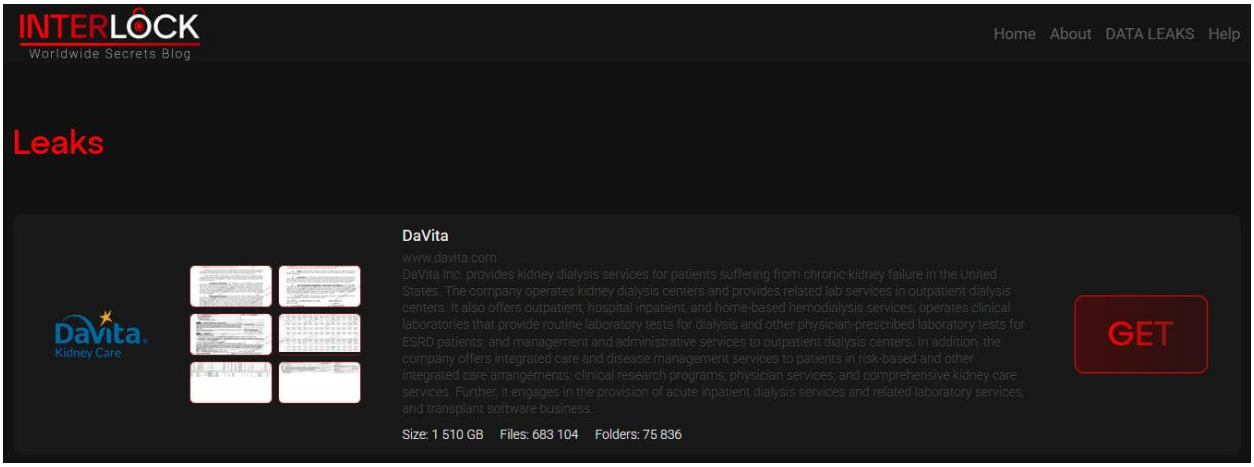
[16] *Id.*

[17] *Form 8-K*, DaVita Inc., United States Securities and Exchange Commission: https://www.sec.gov/Archives/edgar/data/927066/000119312525079593/d948299d8k.htm (last visited July 28, 2025).

[18] *Interlock Ransomware Group Claims Massive 20TB Data Theft from DaVita Healthcare; Millions*, https://www.secureblink.com/cyber-security-news/nterlock-ransomware-group-claims-massive-20-tb-data-theft-from-da-vita-healthcare-millions-of-patients-at-risk (last visited July 28, 2025).

data to pressure organizations into paying ransoms.[19] According to Paul Bischoff, Consumer Privacy Advocate at Comparitech, Interlock successfully executed 13 confirmed cyberattacks and has claimed responsibility for 17 U.S. healthcare breaches in 2025 alone.[20]

43. Upon information and belief, Interlock initially attempted ransom negotiations with DaVita, but those negotiations failed.[21] As a result, on April 24, 2025, Interlock added DaVita to its dark-web "data-leak site" and published the first tranche of files it exfiltrated from DaVita's IT Network.[22]



44. Upon information and belief, the Private Information Interlock published on Plaintiffs and Class Members, includes more than 1.4 million unique Social Security numbers, and other highly sensitive Private Information belonging to Plaintiffs and Class Members.

---

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] Bill Toulas, *Interlock ransomware claims DaVita attacks, leaks stolen data*: https://www.bleepingcomputer.com/news/security/interlock-ransomware-claims-davita-attack-leaks-stolen-data/ (last visited July 28, 2025).

45. DaVita has confirmed that it is aware of Interlock's claims, and that patients Private Information was in fact published on the dark web by the ransomware group.[23]

46. In response to the publication of patients' Private Information, DaVita launched a comprehensive review of the data to identify the exact types of Private Information compromised as well as identify patients affected by the Data Breach.[24]

47. DaVita failed to take precautions designed to keep individuals' Private Information secure.

48. While DaVita sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive Private Information of Plaintiffs and Class Members.

49. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. DaVita Knew the Risks of Storing Valuable Private Information and the Foreseeable Harm to Victims

50. DaVita knew that any breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised, as well as intrusion into their highly private health information.

51. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, Anthem, and many others.

---

[23] https://therecord.media/dialysis-davita-reviewing-data-leak (last visited July 28, 2025).

[24] *The HIPAA Journal*, Ransomware Group Claims Responsibility for DaVita Ransomware Attack; Leaks Data: https://www.hipaajournal.com/davita-ransomware-attack/#:~:text=DaVita%20has%20confirmed%20it%20is,notified%20as%20soon%20as%20possible. (last visited July 28, 2025).

52. Private Information has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the dark web that serve as a bustling marketplace for such commerce."[25] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

53. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the Identity Theft Resource Center ("ITRC"), in 2024, there were 3,158 data breaches, resulting in over 1.7 billion data breach notices, a 312% increase from 2023.[26]

54. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2024, there were 1,135,270 identity theft complaints reported to the FTC and affiliated agencies, a 9.5% increase from 2023.[27] Moreover, in 2024, the FTC received approximately 2.6 million cases of related fraud, with total losses of more than $12.7 billion.[28]

---

[25] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[26] *Data Breach Reports: 2024 End of Year Report*, IDENTITY THEFT RESOURCE CENTER: https://www.idtheftcenter.org/post/2024-annual-data-breach-report-near-record-compromises/#:~:text=According%20to%20the%202024%20Annual,notices%20included%20attack%20vector%20information. (last visited July 28, 2025).

[27] Ben Luthi, *U.S. Fraud and Identity Theft Losses Topped $12.7 Billion in 2024*: https://www.experian.com/blogs/ask-experian/identity-theft-statistics/#:~:text=Source:%20FTC-,Identity%20Theft%20Statistics,260%2C808%20reports%20fielded%20in%202023. (last visited July 28, 2025).

[28] *Id.*

55. The breadth of data believed to be compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiffs and Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

56. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a person's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[29]

57. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[30]

[29] IDExperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows: https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[30] Experian, Healthcare Data Breach: What to Know About them and What to Do After One: https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

58. Compared to other types of personal data, medical records maintain high value on the dark web since they include full identities, insurance details, and treatment history, with a single medical record selling as high as $1,000.[31]

59. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n 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 has been sold or posted on the [Dark] 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."[32]

60. Even if stolen Private Information does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

61. DaVita knew the importance of safeguarding Plaintiffs and Class Members Private Information given the well-publicized rise in data breaches but failed to ensure DaVita deployed adequate data security.

62. Additionally, as a healthcare entity in possession of individuals' Private Information, DaVita knew or should have known the importance of safeguarding the Private

[31] Juan Hernandez, *Dark web threats in healthcare: understanding the risks*: https://preyproject.com/blog/dark-web-threats-in-healthcare (last visited July 28, 2025).

[32] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf.

Information entrusted to it, directly and indirectly, and of the foreseeable consequences of maintaining inadequate data security. Such consequences include the significant costs imposed on Plaintiffs and Class Members due to their Private Information's disclosure to cybercriminals.

D. DaVita Breached its Duty to Protect Patients' Private Information

63. DaVita agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA"). Under state and federal law, businesses like DaVita have duties to protect its patients' Private Information and to notify them about breaches.

64. The Private Information held by DaVita in its computer system and network included the highly sensitive Private Information of Plaintiffs and Class Members.

65. The Data Breach occurred as a direct result of DaVita's failure to implement and follow basic security procedures in order to protect its consumers' Private Information.

E. Plaintiffs and Class Members Suffered Damages

66. For the reasons mentioned above, DaVita's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways. Plaintiffs and Class Members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing

attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

67. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of DaVita's conduct. Further, the value of Plaintiffs and Class Members' Private Information has been diminished by its exposure in the Data Breach.

68. As a result of DaVita's failures, Plaintiffs and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of Private Information.

69. From one study, 28% of consumers affected by a data breach become victims of identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[33]

70. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[34]

71. "Actors buying and selling Private Information from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[35]

[33] https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.

[34] https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud.

[35] *Id.*

72. The reality is that cybercriminals seek nefarious outcomes from a data breach" and "stolen health data can be used to carry out a variety of crimes."[36]

73. Health information in particular is likely to be used in detrimental ways – by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[37]

74. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[38]

75. Plaintiffs and Class Members have also been injured by DaVita's unauthorized disclosure of their confidential and Private Information.

76. Plaintiffs and Class Members are also at a continued risk because their information remains in DaVita's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as DaVita fail to undertake the necessary and appropriate security and training measures to protect its consumers' Private Information.

COMMON INJURIES AND DAMAGES

77. As result of DaVita's ineffective and inadequate data security practices, Plaintiffs and Class Members now face a present and ongoing risk of fraud and identity theft.

[36] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

[37] *Id.*

[38] https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

78. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including but not limited to: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of their Private Information; and (i) the continued risk to their Private Information, which remains in DaVita's possession, and which is subject to further breaches, so long as DaVita fails to undertake appropriate and adequate measures to protect Plaintiffs and Class Members' Private Information.

A. The Risk of Identity Theft to Plaintiffs and Class Members is Present and Ongoing

79. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

80. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

81. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

82. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[39] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[40] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

83. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the Private Information at issue here.[41] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical

[39] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

[40] *Id.*

[41] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[42] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[43]

84. Social Security numbers, for example, are among the worst kinds of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[44]

85. What's more, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

[42] *Id.; What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

[43] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

[44] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

86. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[45]

87. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[46]

88. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[47]

89. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.,* patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to

[45] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[46] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[47] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, Private Information is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the healthcare industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

90. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[48] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[49] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[50]

91. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[51]

92. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[52]

---

[48] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/

[49] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/

[50] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/

[51] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited July 28, 2025).

[52] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/

93. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[53] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[54]

94. One such example of criminals using Private Information for profit is the development of "Fullz" packages. Cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

95. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find

[53] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/

[54] *Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One,* EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-toknow-about-them-and-what-to-do-after-one/ (last visited July 28, 2025).

that Plaintiffs and Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

96. According to the FBI's Internet Crime Complaint Center (IC3) 2024 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $16.6 billion in losses to individuals and business victims.[55]

97. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

98. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

99. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiffs and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

100. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and

[55] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf (last visited July 28, 2025).

amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[56]

101. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[57]

102. According to the FTC, unauthorized PHI disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.[58]

103. DaVita's failure to timely notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs and Class Members' injury by depriving them of the earliest ability to take

---

[56] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

[57] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

[58] *See, e.g.*, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices.

appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

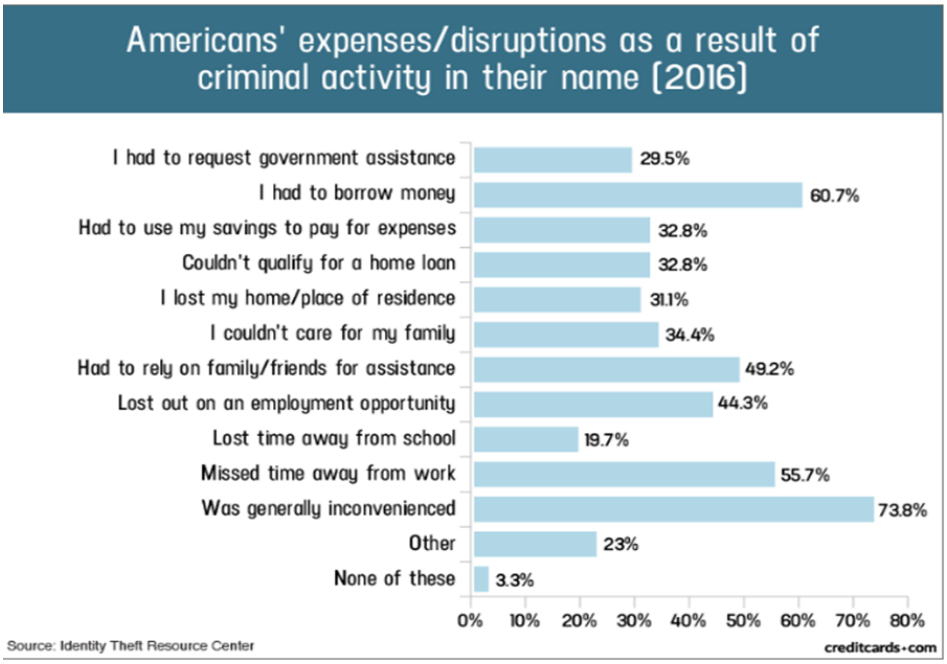
B. Loss of Time to Mitigate the Risk of Identify Theft and Fraud

104. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

105. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

106. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[59]

[59] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.



107. In the event that Plaintiffs and Class Members experience actual identity theft and fraud, they will face substantial costs and time to repair the damage to their good name and credit record.[60] Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[61]

[60] Mark Birchall, *9 consequences of identity theft and how to deal with them*: 9 consequences of identity theft + how to deal with them (last visited July 28, 2025).

[61] *See* https://www.identitytheft.gov/Steps.

C. Diminution of Value of the Private Information

108. Private Information is a valuable property right.[62] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

109. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed Private Information to adjust their insureds' medical insurance premiums.

110. Private Information can sell for as much as $4,000 per record according to the Dark Web Price Index by Privacy Affairs.[63]

111. Medical information is especially valuable to identity thieves. A single medical record can for as high as $1,000 on the dark web.[64]

112. An active and robust legitimate marketplace for Private Information also exists. In 2024, the data brokering industry was worth roughly $70 billion.[65] In fact, the data marketplace is

---

[62] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[63] Ben Luthi, *Here's What Your Data Sells for on the Dark Web*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited July 28, 2025).

[64] Juan Hernandez, *Dark web threats in healthcare: understanding the risks*: https://preyproject.com/blog/dark-web-threats-in-healthcare (last visited July 28, 2025).

[65] https://www.maximizemarketresearch.com/market-report/global-data-broker-market/55670/ (last visited July 28, 2025).

so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[66, 67] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[68]

113. As a result of the Data Breach, Plaintiffs and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the dark web, where it may soon be available and holds significant value for the threat actors.

D. Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary

114. To date, DaVita has done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach.

115. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

116. Such fraud may go undetected until debt collection calls commence months, or even years later. An individual may not know that her or her Social Security Number was used to file

[66] https://datacoup.com/ (last visited July 28, 2025).

[67] https://digi.me/what-is-digime/ (last visited July 28, 2025).

[68] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

117. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

118. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from DaVita's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for DaVita's failure to safeguard their Private Information.

E. Loss of Benefit of the Bargain

119. Furthermore, DaVita's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to provide their Private Information, which was a condition precedent to obtain services, and paying DaVita for its services, Plaintiffs, as consumers, understood and expected that they were, in part, paying for services and data security to protect the Private Information required to be collected from them.

120. In fact, DaVita did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains struck with DaVita.

F. Injunctive Relief is Necessary to Protect Against Future Data Breaches

121. Moreover, Plaintiffs and Class Members have an interest in ensuring that Private Information, which is believed to remain in the possession of DaVita, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to,

making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

122. Because of DaVita's failure to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses and lost time. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their Private Information is used;

b. diminution in value of their Private Information;

c. compromise and continuing publication of their Private Information;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identity theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen Private Information; and

h. continued risk to their Private Information —which remains in DaVita's possession—and is thus as risk for futures breaches so long as DaVita fail to take appropriate measures to protect the Private Information.

G. Lack of Compensation

123. Plaintiffs and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

124. As a direct and proximate result of DaVita's conduct, Plaintiffs and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

125. Further, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach and face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

126. Specifically, many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

e. Addressing their inability to withdraw funds linked to compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Placing “freezes” and “alerts” with credit reporting agencies;

h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. Contacting financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

127. Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

128. DaVita's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of Private Information. Early notification helps a victim of a Data Breach mitigate their injuries, and conversely, delayed notification causes more harm and increases the risk of identity theft. Here, DaVita knew of the breach and waited to formally notify victims. They have yet to explain the delay. This delay violates HIPAA and other notification requirements and increases the injuries to Plaintiffs and Class Members.

H. Plaintiffs' Experiences

Plaintiff Julian Jenkins

129. Plaintiff Jenkins is a patient of DaVita, Inc.

130. DaVita maintained Jenkins's Private Information in its systems at the time of the Data Breach.

131. Plaintiff Jenkins provided his Private Information to DaVita as a condition of receiving health care services, including his Social Security number, date of birth, health insurance information, health payment information, and other medical and health information.

132. Plaintiff Jenkins is careful about sharing his sensitive Private Information. Plaintiff Jenkins stores any documents containing his Private Information in a safe and secure location.

133. Plaintiff Jenkins has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

134. As a result of the Data Breach, Plaintiff Jenkins is at present risk and will continue to be at increased risk of identity theft and fraud for years to come, especially given that the breach included his Social Security number and protected health information.

135. Plaintiff Jenkins has suffered additional actual injuries from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in DaVita's possession and is subject to further unauthorized disclosures so long as DaVita fails to undertake appropriate and adequate measures to protect the Private Information.

136. Moreover, the Data Breach represents a serious invasion of Plaintiff's privacy because the disclosure was to the exact group of people from whom the cybersecurity measures

are supposed to protect Plaintiff and the Class. Moreover, the Private Information has additionally been disseminated to even further cybercriminals.[69]

137. Mr. Jenkins has recently received suspicious text messages about a non-existent medical appointment, and several emails reflecting that he applied for credit for which he did not in fact apply.

138. As a result of the Data Breach and because of the disclosure to cybercriminals, Plaintiff Jenkins will be required to spend considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Indeed, he has already spent several hours researching the breach, reviewing his bank accounts, monitoring his credit report, changing passwords, and other efforts as recommended by experts.

139. Since the Data Breach, and because of the significant risk of identity theft and fraud, Plaintiff has suffered stress and anxiety.

140. As a result of the Data Breach, Plaintiff Jenkins is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come that requires years of credit monitoring and identity theft protection.

141. Plaintiff Jenkins has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in DaVita's possession, is protected and safeguarded from future breaches.

Plaintiff Lydia Perryman

142. Plaintiff Perryman is a current patient of DaVita, Inc. She has received medical treatment on several occasions since April 2023.

[69] https://therecord.media/dialysis-davita-reviewing-data-leak.

143. Plaintiff Perryman recently contacted DaVita regarding her treatment and was told by DaVita's staff that unauthorized third parties had gained access to DaVita's computer systems and that such systems were inoperative as a result.

144. DaVita maintained Perryman's Private Information in its systems at the time of the Data Breach.

145. Plaintiff Perryman provided her Private Information to DaVita as a condition of receiving health care services, including her Social Security number, date of birth, health insurance information, health payment information, and other medical and health information.

146. Plaintiff Perryman is careful about sharing her sensitive Private Information. Plaintiff Perryman stores any documents containing her Private Information in a safe and secure location.

147. Plaintiff Perryman has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

148. As a result of the Data Breach, Plaintiff Perryman is at present risk and will continue to be at increased risk of identity theft and fraud for years to come, especially given that the breach included her Social Security number and protected health information.

149. Plaintiff Perryman has suffered additional actual injuries from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available

for unauthorized third parties to access and abuse; and (b) remains backed up in DaVita's possession and is subject to further unauthorized disclosures so long as DaVita fails to undertake appropriate and adequate measures to protect the Private Information.

150. Moreover, the Data Breach represents a serious invasion of Plaintiff's privacy because the disclosure was to the exact group of people from whom the cybersecurity measures are supposed to protect Plaintiff and the Class. Moreover, the Private Information has additionally been disseminated to even further cybercriminals.[70]

151. Plaintiff has also experienced a significant increase in spam calls and messages since the data breach.

152. As a result of the Data Breach and because of the disclosure to cybercriminals, Plaintiff Perryman will be required to spend considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Indeed, she has already spent several hours researching the breach, reviewing her bank accounts, monitoring her credit report, changing passwords, and other efforts as recommended by experts.

153. Since the Data Breach, and because of the significant risk of identity theft and fraud, Plaintiff has suffered stress and anxiety.

154. As a result of the Data Breach, Plaintiff Perryman is at present risk and will continue to be at increased risk of identity theft and fraud for years to come that requires years of credit monitoring and identity theft protection.

[70] https://therecord.media/dialysis-davita-reviewing-data-leak.

155. Plaintiff Perryman has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in DaVita's possession, is protected and safeguarded from future breaches.

Plaintiff Brenda Pearson

156. Plaintiff Pearson is a current patient of DaVita, Inc. She visits DaVita's facilities approximately every two to three months for dialysis treatment.

157. DaVita maintained Pearson's Private Information in its systems at the time of the Data Breach.

158. Plaintiff Pearson provided her Private Information to DaVita as a condition of receiving health care services, including her Social Security number, date of birth, health insurance information, health payment information, and other medical and health information.

159. Plaintiff Pearson is careful about sharing her sensitive Private Information. Plaintiff Pearson stores any documents containing her Private Information in a safe and secure location.

160. Plaintiff Pearson has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

161. As a result of the Data Breach, Plaintiff Pearson is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come, especially given that the breach included her Social Security number and protected health information.

162. Plaintiff Pearson has suffered additional actual injuries from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences

of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in DaVita's possession and is subject to further unauthorized disclosures so long as DaVita fails to undertake appropriate and adequate measures to protect the Private Information.

163. Moreover, the Data Breach represents a serious invasion of Plaintiff's privacy because the disclosure was to the exact group of people from whom the cybersecurity measures are supposed to protect Plaintiff and the Class. Moreover, the Private Information has additionally been disseminated to even further cybercriminals.[71]

164. Plaintiff has also experienced a significant increase in spam calls and messages since the data breach.

165. As a result of the Data Breach and because of the disclosure to cybercriminals, Plaintiff Pearson will be required to spend considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Indeed, she has already spent several hours researching the breach, reviewing her bank accounts, monitoring her credit report, changing passwords, and other efforts as recommended by experts.

166. Since the Data Breach, and because of the significant risk of identity theft and fraud, Plaintiff has suffered stress and anxiety.

167. As a result of the Data Breach, Plaintiff Pearson is at present risk and will continue to be at increased risk of identity theft and fraud for years to come, which requires years of credit monitoring and identity theft protection.

[71] https://therecord.media/dialysis-davita-reviewing-data-leak.

168. Plaintiff Pearson has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in DaVita's possession, is protected and safeguarded from future breaches.

Plaintiff G.I.

169. Plaintiff G.I. is a patient of DaVita, Inc. He visited DaVita's facilities in Missouri approximately for 13 months from March 2023 to April 2024.

170. DaVita maintained G.I.'s Private Information in its systems at the time of the Data Breach.

171. Plaintiff G.I. provided his Private Information to DaVita as a condition of receiving health care services, including his Social Security number, date of birth, health insurance information, health payment information, and other medical and health information.

172. Plaintiff G.I. is careful about sharing his sensitive Private Information. Plaintiff G.I. stores any documents containing her Private Information in a safe and secure location.

173. Plaintiff G.I. has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

174. As a result of the Data Breach, Plaintiff G.I. is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come, especially given that the breach included his Social Security number and protected health information.

175. Plaintiff G.I. has suffered additional actual injuries from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences

of the Data Breach; (vi) statutory damages; (vii) lost medical expenses; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in DaVita's possession and is subject to further unauthorized disclosures so long as DaVita fails to undertake appropriate and adequate measures to protect the Private Information.

176. The Data Breach represents a serious invasion of Plaintiff's privacy because the disclosure was to the exact group of people from whom the cybersecurity measures are supposed to protect Plaintiff and the Class. Moreover, the Private Information has additionally been disseminated to even further cybercriminals.[72]

177. Plaintiff has also experienced a significant increase in spam calls and messages since the data breach.

178. As a result of the Data Breach and because of the disclosure to cybercriminals, Plaintiff G.I. will be required to spend considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Indeed, she has already spent several hours researching the breach, reviewing his bank accounts, monitoring his credit report, changing passwords, and other efforts as recommended by experts.

179. Since the Data Breach, and because of the significant risk of identity theft and fraud, Plaintiff has suffered stress and anxiety.

180. As a result of the Data Breach, Plaintiff G.I. is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come, which requires years of credit monitoring and identity theft protection.

[72] https://therecord.media/dialysis-davita-reviewing-data-leak.

181. Plaintiff G.I. has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in DaVita's possession, is protected and safeguarded from future breaches.

Plaintiff Anthony Natoli

182. Plaintiff Natoli is a patient of DaVita, Inc.

183. DaVita maintained Plaintiff Natoli's Private Information in its systems at the time of the Data Breach.

184. Plaintiff Natoli provided his Private Information to DaVita as a condition of receiving health care services, including his Social Security number, date of birth, health insurance information, health payment information, and other medical and health information.

185. Plaintiff Natoli is careful about sharing his sensitive Private Information. Plaintiff Natoli stores any documents containing his Private Information in a safe and secure location.

186. Plaintiff Natoli has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

187. As a result of the Data Breach, Plaintiff Natoli is at present risk and will continue to be at increased risk of identity theft and fraud for years to come, especially given that the breach included his Social Security number and protected health information.

188. Plaintiff Natoli has suffered additional actual injuries from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and

certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in DaVita's possession and is subject to further unauthorized disclosures so long as DaVita fails to undertake appropriate and adequate measures to protect the Private Information.

189. Moreover, the Data Breach represents a serious invasion of Plaintiff's privacy because the disclosure was to the exact group of people from whom the cybersecurity measures are supposed to protect Plaintiff and the Class. Moreover, the Private Information has additionally been disseminated to even further cybercriminals.[73]

190. Plaintiff has also experienced a significant increase in spam calls and messages since the data breach.

191. As a result of the Data Breach and because of the disclosure to cybercriminals, Plaintiff Natoli will be required to spend considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Indeed, he has already spent several hours researching the breach, reviewing his bank accounts, monitoring his credit report, changing passwords, and other efforts as recommended by experts.

192. Since the Data Breach, and because of the significant risk of identity theft and fraud, Plaintiff has suffered stress and anxiety.

193. As a result of the Data Breach, Plaintiff Natoli is at present risk and will continue to be at increased risk of identity theft and fraud for years to come, which requires years of credit monitoring and identity theft protection.

[73] https://therecord.media/dialysis-davita-reviewing-data-leak.

194. Plaintiff Natoli has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in DaVita's possession, is protected and safeguarded from future breaches.

Plaintiff Gregory Leafe

195. Plaintiff Leafe is a patient of DaVita, Inc.

196. DaVita maintained Plaintiff Leafe's Private Information in its systems at the time of the Data Breach.

197. Plaintiff Leafe provided his Private Information to DaVita as a condition of receiving health care services, including his Social Security number, date of birth, health insurance information, health payment information, and other medical and health information.

198. Plaintiff Leafe is careful about sharing his sensitive Private Information. Plaintiff Leafe stores any documents containing his Private Information in a safe and secure location.

199. Plaintiff Leafe has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

200. As a result of the Data Breach, Plaintiff Leafe is at present risk and will continue to be at increased risk of identity theft and fraud for years to come, especially given that the breach included his Social Security number and protected health information.

201. Plaintiff Leafe has suffered additional actual injuries from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and

certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in DaVita's possession and is subject to further unauthorized disclosures so long as DaVita fails to undertake appropriate and adequate measures to protect the Private Information.

202. Moreover, the Data Breach represents a serious invasion of Plaintiff's privacy because the disclosure was to the exact group of people from whom the cybersecurity measures are supposed to protect Plaintiff and the Class. Moreover, the Private Information has additionally been disseminated to even further cybercriminals.[74]

203. Plaintiff has also experienced a significant increase in spam calls and messages since the data breach.

204. As a result of the Data Breach and because of the disclosure to cybercriminals, Plaintiff Leafe will be required to spend considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Indeed, he has already spent several hours researching the breach, reviewing his bank accounts, monitoring his credit report, changing passwords, and other efforts as recommended by experts.

205. Since the Data Breach, and because of the significant risk of identity theft and fraud, Plaintiff has suffered stress and anxiety.

206. As a result of the Data Breach, Plaintiff Leafe is at present risk and will continue to be at increased risk of identity theft and fraud for years to come, which requires years of credit monitoring and identity theft protection.

[74] https://therecord.media/dialysis-davita-reviewing-data-leak.

207. Plaintiff Leafe has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in DaVita's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

208. Plaintiffs bring this action on behalf of themselves, and all other persons similarly situated pursuant to Fed. R. Civ. P. 23(a) and (b) (the "Nationwide Class"):

All United States residents whose PII and/or PHI was compromised in the Data Breach.

209. Plaintiffs Natoli and Leafe bring this action on behalf of themselves, and all other persons similarly situated pursuant to Fed. R. Civ. P. 23(a) and (b) (the "California Class"):

All California residents whose PII and/or PHI were compromised in the Data Breach.

210. Plaintiff Perryman brings this action on behalf of herself, and all other persons similarly situated pursuant to Fed. R. Civ. P. 23(a) and (b) (the "Arizona Class"):

All Arizona residents whose PII and/or PHI were compromised in the Data Breach.

211. Plaintiff Pearson brings this action on behalf of herself, and all other persons similarly situated pursuant to Fed. R. Civ. P. 23(a) and (b) (the "North Carolina Class"):

All North Carolina residents whose PII and/or PHI were compromised in the Data Breach.

212. Excluded from the Classes are DaVita, any entity in which DaVita has a controlling interest, and DaVita's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Classes are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

213. Plaintiffs reserve the right to modify or amend the definitions of the proposed Classes as additional information becomes available to Plaintiffs.

214. **Numerosity:** The Classes are so numerous that individual joinder of all Class Members is impracticable. Plaintiffs have good reason to believe that the Data Breach has exposed

the Private Information of at least 1.2 million individuals. All Class Members' names and addresses are available from DaVita's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

215. **Commonality:** There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether and to what extent DaVita had a duty to protect the Private Information of Class Members;

b. Whether DaVita was negligent in collecting and storing Plaintiffs' and Class Members' Private Information;

c. Whether DaVita had duties not to disclose the Private Information of Class Members to unauthorized third parties;

d. Whether DaVita took reasonable steps and measures to safeguard Plaintiffs' and Class Members' Private Information;

e. Whether DaVita failed to adequately safeguard the Private Information of Class Members;

f. Whether DaVita failed to implement and maintain reasonable security policies and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether DaVita adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

h. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or punitive damages because of DaVita's wrongful conduct;

i. Whether Plaintiffs and Class Members are entitled to restitution because of DaVita's wrongful conduct;

j. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm they face because of the Data Breach; and

k. Whether Plaintiffs and Class Members are entitled to identity theft protection for their respective lifetimes.

216. **Typicality:** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was disclosed by DaVita. Plaintiffs' claims are typical of those of the other Class Members because, inter alia, all Class Members were injured through DaVita's common misconduct. Plaintiffs are advancing the same claims and legal theories individually and on behalf of all other Class Members, and there are no defenses that are unique to Plaintiff. Plaintiffs' claims and Class Members' claims arise from the same operative facts and are based on the same legal theories.

217. **Adequacy:** Plaintiffs are adequate representatives of the Classes because Plaintiffs are members of the Classes they seek to represent, and are committed to pursuing this matter against DaVita to obtain relief for the Classes. Plaintiffs have no conflicts of interest with the Classes. Plaintiffs' counsel are competent and experienced in litigating class actions, including extensive experience in data breach litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Classes' interests.

218. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because DaVita has acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Classes as a whole. DaVita's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on DaVita's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

219. **Superiority:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a

large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like DaVita. Even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

220. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because DaVita would necessarily gain an unconscionable advantage in non-class litigation, since DaVita would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by Class Members and will establish the right of each Class Member to recover on the causes of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

221. The litigation of Plaintiffs' claims is manageable. DaVita's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with maintenance of this lawsuit as a class action.

222. Adequate notice can be given to Class Members directly using information maintained in DaVita's records.

223. Unless a class-wide injunction is issued, DaVita may continue to maintain inadequate security with respect to the Private Information of Class Members, DaVita may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and DaVita may continue to act unlawfully as set forth in this Complaint.

224. DaVita has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

COUNT I
NEGLIGENCE
(on behalf of Plaintiffs and the Nationwide Class)

225. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

226. DaVita knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. That duty included, among other things, designing, maintaining, and testing DaVita's security protocols to ensure that Plaintiffs' and Class Members' Private Information in DaVita's possession was adequately secured and protected, that Plaintiffs' and Class Members' Private Information on DaVita's networks was not accessible to criminals without authorization, and that DaVita's employees tasked with maintaining such information were adequately trained on security measures regarding the security of Plaintiffs' and Class Members' Private Information.

227. Plaintiffs and Class Members entrusted their Private Information to DaVita with the understanding that DaVita would safeguard their information, use their Private Information for business purposes only, and not disclose their Private Information to unauthorized third parties.

228. DaVita knew or reasonably should have known that a failure to exercise due care in the collecting, storing, and using Plaintiffs' and Class Members' Private Information involved an unreasonable risk of harm to Plaintiffs and Class Members.

229. DaVita also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' Private Information.

230. A breach of security, unauthorized access, and resulting injury to Plaintiffs and Class Members was reasonably foreseeable, particularly in light of prior data breaches and disclosures prevalent in today's digital landscape.

231. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. DaVita knew or should have known of the inherent risks in collecting and storing Plaintiffs' and Class Members' Private Information, the critical importance of providing adequate security of that information, the necessity for encrypting Private Information stored on DaVita's systems, and that it had inadequate IT security protocols in place to secure Plaintiffs' and Class Members' Private Information.

232. DaVita's misconduct created a foreseeable risk of harm to Plaintiffs and Class Members. DaVita's misconduct included, but was not limited to, failure to take the steps and opportunities to prevent the Data Breach as set forth herein.

233. Plaintiffs and Class Members had no ability to protect their Private Information that was in DaVita's possession.

234. DaVita was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

235. DaVita had, and continues to have, a duty to timely disclose that Plaintiffs' and Class Members' Private Information within its possession was compromised and precisely the type(s) of information that were compromised.

236. DaVita had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' Private Information.

237. DaVita systematically failed to provide adequate security for data in its possession.

238. DaVita, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within its possession.

239. DaVita, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' Private Information.

240. DaVita, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiffs and Class Members that the Private Information within its possession might have been compromised and precisely the type of information compromised.

241. DaVita's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised.

242. But for all of DaVita's acts of negligence detailed above, including allowing cyber criminals to access its systems containing Plaintiffs' and Class Members' Private Information would not have been compromised.

243. Plaintiffs never transmitted their own unencrypted Private Information over the internet or any other unsecured source.

244. Following the Data Breach, Plaintiffs' Private Information has been seized by unauthorized third parties who are now free to exploit and misuse that Private Information, and Plaintiffs are unable to prevent its further dissemination. Plaintiffs' Private Information are forever compromised.

245. But for the Data Breach, Plaintiffs would not have incurred the loss and publication of their PII and PHI and other injuries.

246. There is a close causal connection between DaVita's failure to implement security measures to protect Plaintiffs' and Class Members' Private Information and the harm suffered, or risk of imminent harm suffered by Plaintiffs and Class Members. Plaintiffs' and Class Members' Private Information were accessed and compromised as the proximate result of DaVita's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures and encryption.

247. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, loss of privacy, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

248. As a result of DaVita's negligence and breach of duties, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which are still in the possession of third parties, will be used for fraudulent purposes.

249. Plaintiffs seek the award of actual damages on behalf of themselves and the Class.

250. Plaintiffs seek injunctive relief on behalf of the Class in the form of an order (1) compelling DaVita to institute appropriate data collection and safeguarding methods and policies with regard to Private Information; and (2) compelling DaVita to provide detailed and specific

disclosure of what types of Private Information have been compromised as a result of the data breach.

COUNT II
NEGLIGENCE *PER SE*
(on behalf of Plaintiffs and the Nationwide Class)

251. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

252. Under the FTC Act, 15 U.S.C. § 45, DaVita had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

253. Section 5 of the 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 DaVita, of failing to use reasonable measures to protect the Private Information entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of DaVita's duty to protect Plaintiffs and Class Members' Private Information.

254. The FTC has promulgated a clear standard of care expected to comply with Section 5 of the FTC Act through its guidance documents and the many consent orders requiring the implementation of specific cybersecurity safeguards as part of FTC enforcement actions after data breaches.

255. DaVita breached its respective duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their Private Information.

256. DaVita violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. DaVita's conduct was particularly unreasonable given the nature and amount of Private

Information DaVita had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach.

257. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because 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 Class Members.

258. But for DaVita's wrongful and negligent breach of its duties owed, Plaintiffs and Class Members would not have been injured.

259. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of DaVita's breach of its duties. DaVita knew or should have known that it was failing to meet its duties and that the Data Breach would cause Plaintiffs and Class Members to suffer the foreseeable harms associated with the exposure of their Private Information.

260. Similarly, HIPAA imposes on DaVita a duty to follow HIPAA standards for privacy and security practices so as to protect Plaintiffs' and Class Members' PHI.

261. DaVita violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with the applicable regulations detailed above. DaVita's conduct was particularly unreasonable given the nature and amount of PHI that DaVita collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach.

262. DaVita's various violations and its failure to comply with applicable laws and regulations constitutes negligence per se.

263. As a direct and proximate result of DaVita's negligence per se, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries.

COUNT III
BREACH OF IMPLIED CONTRACT
(on behalf of Plaintiffs and the Nationwide Class)

264. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

265. As a condition of obtaining services from DaVita, Plaintiffs and Class Members were obligated to provide their Private Information to DaVita.

266. In so doing, Plaintiffs and Class Members entered into implied contracts with DaVita by which DaVita agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

267. Plaintiffs and Class Members paid directly or indirectly for DaVita's services, and fully performed their obligations under the implied contracts with DaVita.

268. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that DaVita's data and cybersecurity practices and policies were reasonable and consistent with industry standards. Plaintiffs and Class Members believed that DaVita would use part of the money paid to DaVita to fund adequate and reasonable data and cybersecurity practices.

269. Plaintiffs and Class Members would not have provided and entrusted their sensitive and confidential information to DaVita in the absence of the implied contract or implied terms between them and DaVita. The safeguarding of Plaintiffs' and Class Members' Private Information was critical to realize the intent of the parties.

270. DaVita breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their Private Information.

271. As a direct and proximate result of DaVita's breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) 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 confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

272. As a direct and proximate result of DaVita's described breach of implied contract, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT IV
VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT ("CMIA")
CAL. CIV. CODE § 56.101
(on behalf of Plaintiffs Natoli and Leafe and the California Class)

273. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

274. DaVita is a "provider of health care" as defined in Civil Code § 56.06. DaVita is organized for the purpose of providing healthcare. DaVita provides healthcare services to citizens of California.

275. Plaintiffs Natoli and Leafe and California Class Members are "patients" within the meaning of California Civil Code § 56.05(l).

276. Plaintiffs Natoli and Leafe and California Class Members, as patients, had their individually identifiable "medical information," within the meaning of California Civil Code §

56.05(i), created, maintained, preserved, stored, abandoned, destroyed, or disposed of on or through DaVita's computer networks at the time of the Data Breach.

277. DaVita violated California Civil Code § 56.101 by failing to maintain and preserve the confidentiality of Plaintiffs Natoli and Leafe and California Class Members' medical information.

278. In violation of California Civil Code § 56.101(a), DaVita negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs Natoli and Leafe and California Class Members' medical information in a manner that failed to preserve the security of that information and breached its confidentiality. As a result, Plaintiffs Natoli and Leafe and California Class Members' confidential information and records were negligently obtained by hackers in the Data Breach.

279. Medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as defined by California Civil Code § 56.101(c).

280. That the information obtained in the breach was viewed by unauthorized individuals is evidenced by the fact that the personal information was exfiltrated by hackers.

281. In violation of California Civil Code § 56.101(b)(1)(A), DaVita's electronic health record systems or electronic medical record systems failed to protect and preserve the integrity of electronic medical information.

282. DaVita also violated California Civil Code §56.36(b) by negligently releasing Plaintiffs Natoli and Leafe and California Class Members' confidential information in the Data Breach.

283. DaVita's wrongful conduct, actions, inaction, omissions, and want of ordinary care violated the CMIA and directly and proximately caused the Data Breach. Plaintiffs Natoli and

Leafe and California Class Members consequently have suffered (and will continue to suffer) economic damages and other injuries and actual harm including, without limitation: (1) the compromise and theft of their medical information; (2) loss of the opportunity to control how their medical information is used; (3) diminution in the value and use of their medical information entrusted to DaVita with the understanding that DaVita would safeguard it against theft and not allow it to be accessed and misused by third parties; (4) out-of-pocket costs associated with the prevention and detection of, and recovery from, identity theft and misuse of their medical information; (5) continued undue risk to their medical information; and (6) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their medical information being stolen in the Data Breach.

284. Plaintiffs Natoli and Leafe and California Class Members were injured and have suffered damages, as described above, from DaVita's negligent release of their medical information in violation of California Civil Code §§ 56.36, and 56.101, and accordingly are entitled to relief under California Civil Code 56.36, including actual damages, nominal statutory damages of $1,000, injunctive relief, and attorney fees, expenses, and costs.

COUNT V
VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT
CAL. CIV. CODE § 1798.100, *et seq*. ("CCPA")
(on behalf of Plaintiffs Natoli and Leafe and the California Class)

285. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

286. In 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. The CCPA imposes a duty on businesses that maintain personal information of California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the

information collected. DaVita failed to implement the appropriate procedures which resulted in the Data Breach.

287. The CCPA also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

288. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper."

289. Plaintiffs Natoli and Leafe and California Class Members are "consumer[s]" as defined by Cal. Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in § 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

290. DaVita is a "business" as defined by Civ. Code § 1798.140(c) because DaVita:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners;"

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information;"

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

291. The Private Information compromised in the Data Breach is personal information as defined by California Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiffs Natoli and Leafe and California Class Members' names and Social Security numbers.

292. Plaintiffs Natoli and Leafe and California Class Members' Private Information was subject to unauthorized access and exfiltration, theft, or disclosure because their personal information, including name and contact information, was unlawfully accessed, viewed and obtained by an unauthorized third party.

293. The Data Breach occurred as a result of DaVita's failure to implement and maintain reasonable security procedures and practices appropriate to protect the Private Information of Plaintiffs Natoli and Leafe and California Class Members. DaVita failed to implement reasonable security procedures to prevent an attack on its server, including its email system, by hackers and to prevent unauthorized access of Plaintiffs Natoli and Leafe and California Class Members' Private Information as a result of this attack.

294. On July 28, 2025, Plaintiff Natoli provided DaVita with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). On July 30, 2025, Plaintiff Leafe provided DaVita with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). If DaVita has not cured the violation within 30 days thereof, Plaintiffs will amend this Complaint to seek all relief available under the CCPA, including damages to be measured as the greater of actual damages or statutory damages in an amount up to $750 per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

295. As a result of DaVita's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiffs Natoli and Leafe now seek injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by this Court.

COUNT VI
VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW
CAL. CIV. CODE § 17200, *et seq*. ("UCL")
(on behalf of Plaintiffs Natoli and Leafe and the California Class)

296. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

297. The California Unfair Competition Law, Cal. Bus. & Prof. Code sections 17200 *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

298. By reason of DaVita's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiffs Natoli and Leafe and California Class Members' Private Information, DaVita engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.

299. DaVita has violated the UCL by engaging in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to Plaintiffs Natoli and Leafe and California Class Members.

300. DaVita's business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers, in that Plaintiffs Natoli and Leafe California Class Members' Private Information has been compromised for unauthorized parties to see, use, and otherwise exploit.

301. DaVita's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs Natoli and Leafe and California Class Members' Private Information also constitute "unfair" business acts and practices within the meaning of Business & Professions Code sections 17200 *et seq*., in that DaVita's conduct was substantially injurious to Plaintiffs Natoli and Leafe and California Class Members, offensive to public policy, immoral, unethical, oppressive and unscrupulous, and the gravity of DaVita's conduct outweighs any alleged benefits attributable to such conduct.

302. DaVita engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs Natoli and Leafe and California Class Members' Private Information with knowledge that the information would not be adequately protected; by violating the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56.101(a); by violating the other statutes described above; and by storing Plaintiffs Natoli and Leafe and California Class Members' PII and PHI in an unsecure electronic environment in violation of HIPAA and California's data

breach statute, Cal. Civ. Code § 1798.81.5, which require DaVita to take reasonable methods of safeguarding Plaintiffs Natoli and Leafe and California Class Members' Private Information.

303. DaVita's practices were also unlawful and in violation of Civil Code sections 1798 *et seq*. and DaVita's own privacy policy because DaVita failed to take reasonable measures to protect Plaintiffs Natoli and Leafe and California Class Members' Private Information, and failed to take remedial measures such as notifying its users when it first discovered that their Private Information may have been compromised.

304. In addition, DaVita engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82 and Cal. Health & Safety Code §1280.15(b)(2).

305. DaVita's business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the Private Information they provided to DaVita will remain private and secure, when in fact it has not been maintained in a private and secure manner, and that DaVita would take proper measures to investigate and remediate a data breach, when DaVita did not do so.

306. Plaintiffs Natoli and Leafe and California Class Members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of DaVita's above-described wrongful actions, inaction, and omissions including, *inter alia*, the unauthorized release and disclosure of their Private Information and lack of notice.

307. But for DaVita's misrepresentations and omissions, Plaintiffs Natoli and Leafe and California Class Members would not have provided their Private Information to DaVita, or would have insisted that their PII and PHI be more securely protected.

308. As a direct and proximate result of DaVita's unlawful practices and acts, Plaintiffs Natoli and Leafe and California Class Members were injured and lost money or property, including but not limited to the price received by DaVita for its services, the loss of Plaintiffs Natoli and Leafe and California Class Members' legally protected interest in the confidentiality and privacy of their Private Information, nominal damages, and additional losses as described herein.

309. DaVita knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs Natoli and Leafe and California Class Members' Private Information and that the risk of a data breach or theft was highly likely. DaVita's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs Natoli and Leafe and California Class Members.

310. Plaintiffs Natoli and Leafe seek prospective injunctive relief, including improvements to DaVita's data security systems and practices, in order to ensure that such security is reasonably sufficient to safeguard patients' Private Information that remains in DaVita's custody, including but not limited to the following:

a. Ordering that DaVita engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on DaVita's systems on a periodic basis, and ordering DaVita to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that DaVita engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that DaVita audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that DaVita segment patient data by, among other things, creating firewalls and access controls so that if one area of DaVita's systems is compromised, hackers cannot gain access to other portions of DaVita's systems;

e. Ordering that DaVita not transmit Private Information via unencrypted email;

f. Ordering that DaVita not store Private Information in email accounts;

g. Ordering that DaVita purge, delete, and destroy in a reasonably secure manner patient data not necessary for provisions of DaVita's services;

h. Ordering that DaVita conduct regular computer system scanning and security checks;

i. Ordering that DaVita routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering DaVita to meaningfully educate its current, former, and prospective patients about the threats they face as a result of the loss of their PII and PHI to third parties, as well as the steps they must take to protect themselves.

311. Unless such Class-wide injunctive relief is issued, Plaintiffs Natoli and Leafe and California Class Members remain at risk, and there is no other adequate remedy at law that would

ensure that Plaintiffs Natoli and Leafe (and other consumers) can rely on DaVita's representations regarding its data security in the future.

312. Furthermore, in the alternative to all legal remedies sought herein, Plaintiffs Natoli and Leafe, on behalf of the California Class, seek monetary relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including but not limited to restitution to Plaintiffs Natoli and Leafe and California Class Members of money or property that DaVita may have acquired by means of its unlawful, and unfair business practices; restitutionary disgorgement of all profits accruing to DaVita because of its unlawful and unfair business practices; declaratory relief; and attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

COUNT VII
VIOLATION OF ARIZONA CONSUMER FRAUD ACT
ARIZ. REV. STAT. § 44-1521, *et seq*.
(on behalf of Plaintiff Perryman and the Arizona Class)

313. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

314. DaVita sold Plaintiff Perryman and the Arizona Class "merchandise" as that term as defined by A.R.S. § 44-1521, in the form of services, including health and insurance services, as well as the provision of other customer care services.

315. Section 44-1522 of the Arizona Consumer Fraud Act provides:

> The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby.

See A.R.S. § 44-1522(A).

316. DaVita used deception, used a deceptive act or practice, and fraudulently omitted and concealed material facts in connection with the sale or advertisement of that merchandise in violation of A.R.S. § 44-1522(A).

317. DaVita omitted and concealed material facts, which it knew about and had the duty to disclose--namely, DaVita's inadequate privacy and security protections for Plaintiff Perryman's and the Arizona Class's Private Information. DaVita omitted and concealed those material facts even though in equity and good conscience they should have been disclosed and did so with the intent that others would rely on the omission, suppression, and concealment.

318. The concealed facts are material in that they are logically related to the transactions at issue and rationally significant to the parties in view of the nature and circumstances of those transactions.

319. Plaintiff Perryman does not allege any claims based on any affirmative misrepresentations by DaVita; rather Plaintiff Perryman alleges that DaVita omitted, failed to disclose and concealed material facts and information as alleged herein, despite its duty to disclose those facts.

320. DaVita knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff Perryman's and the Arizona Class's Private Information, and that the risk of a data breach or theft was highly likely. DaVita's actions in engaging in these deceptive acts and practices were negligent, knowing and willful, and wanton and reckless with respect to the rights of Plaintiff Perryman and the Arizona Class.

321. Plaintiff Perryman and the Arizona Class were ignorant of the truth and the concealed facts and incurred damages as a consequent and proximate result.

322. Plaintiff Perryman and the Arizona Class seek all available relief under A.R.S. § 44-1521, et. seq., including, but not limited to, compensatory damages, punitive damages, injunctive relief, and attorneys' fees and costs.

COUNT VIII
VIOLATION OF NORTH CAROLINA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT
N.C.G.S.A. § 75-1.1, *et seq*.
(on behalf of Plaintiff Pearson and the North Carolina Class)

323. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

324. N.C.G.S.A. § 75-65 provides that any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach.

325. N.C.G.S.A. § 75-65 further provides that the disclosure notification shall be made "without unreasonable delay".

326. N.C.G.S.A. § 75-65 further provides that a violation of that section is a violation of North Carolina's Unfair and Deceptive Trade Practices Act, G.S. § 75-1.1, and that a private right of action may be brought by an individual for a violation if such individual is injured as a result of the violation.

327. DaVita is a business that owns or licenses personal information of residents of North Carolina for the purposes of N.C.G.S.A. § 75-65.

328. Plaintiff Pearson and North Carolina Class Members are residents of North Carolina.

329. DaVita has unreasonably delayed the disclosure notification, as required under N.C.G.S.A. § 75-65. In particular, DaVita still has not provided notice of the Data Breach to Plaintiff Pearson and North Carolina Class Members more than three months after the Data Breach took place.

330. On information and belief, no law enforcement agency has informed DaVita that providing a notification disclosure consistent with N.C.G.S.A. § 75-65 will impede any criminal investigation.

331. By unreasonably delaying the requisite notification disclosure, DaVita has violated N.C.G.S.A. § 75-65 and, in turn, N.C.G.S.A. § 75-1.1.

332. Plaintiff Pearson and North Carolina Class Members have been injured by DaVita's violation of N.C.G.S.A. § 75-65 as alleged herein.

333. Accordingly, Plaintiff Pearson, individually and on behalf of the North Carolina Class, requests that the Court award all relevant damages and reasonable attorneys' fees as allowable by law.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs, individually and on behalf of all others similarly situated, pray for relief as follows:

a. for an Order certifying the Class as defined herein, and appointing Plaintiffs and their counsel to represent the Class;

b. for equitable relief enjoining DaVita from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

c. for equitable relief compelling DaVita to use appropriate cybersecurity methods and policies with respect to Private Information collection, storage, and protection, and to disclose with specificity to Class Members the types of Private Information compromised;

d. for an award of damages, including actual, nominal, consequential, enhanced compensatory, and punitive damages, as allowed by law in an amount to be determined;

e. for an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f. for prejudgment interest on all amounts awarded; and

g. such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: July 30, 2025

Respectfully submitted,

/s/ Bart D. Cohen

Bart D. Cohen
BAILEY GLASSER LLP
1622 Locust Street
Philadelphia, PA 19103
(215) 274-9420
bcohen@baileyglasser.com

J. Gerard Stranch, IV
Grayson Wells
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
(615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

Gary Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
(866) 252-0878
gklinger@milberg.com

Interim Co-Lead Class Counsel

Maureen M. Brady
MCSHANE & BRADY, LLC
4006 Central Street
Kansas City, MO 64111
(816) 888-8010
mbrady@mcshanebradylaw.com

Mark Reich
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
(212) 363-7500
mreich@zlk.com

Marc H. Edelson
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940
(215) 867-2399
medelson@edelson-law.com

Plaintiff's Executive Committee