UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE
SOUTHERN DIVISION

GARY SELF, on behalf of himself and on behalf of all other similarly situated individuals, Plaintiff, v. **NATIONWIDE RECOVERY SERVICE, INC.,** and **HAMILTON HEALTH CARE SYSTEM, INC. D/B/A VITRUVIAN HEALTH**, Defendants.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Gary Self ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Defendant Nationwide Recovery Service, Inc. ("NRS") and Defendant Hamilton Health Care System, Inc. d/b/a Vitruvian Health ("Vitruvian Health") (collectively, "Defendants"), alleging as follows, based upon personal knowledge and investigation of counsel.

I. INTRODUCTION

1. This class action arises from NRS's failure to properly secure and safeguard Plaintiff's and Class Members' confidential protected health information ("PHI")[1] and personally

[1] The Department of Health and Human Services ("HHS") defines "protected health information" as "individually identifiable health information . . . that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103. "Health information" means "any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an

identifiable information ("PII")[2] (collectively, "Private Information"), which as a result, was **stolen** from NRS's systems and is now in the hands of cybercriminals.

2. Between July 5, 2024, and July 11, 2024, an unauthorized actor hacked into NRS's inadequately secured network environment and **exfiltrated** Plaintiff's and Class Members' sensitive, confidential Private Information stored therein, including their names, addresses, Social Security numbers, dates of birth, financial account information, and other medical information, causing widespread injuries and damages to Plaintiff and Class Members ("Data Breach" or "Breach").

3. NRS is a third-party collection agency serving clients across the United States.[3]

4. Vitruvian Health utilized NRS's services.

5. Plaintiff and Class Members are current or former patients of Vitruvian Health.

6. As a condition of receiving Vitruvian Health's services, Plaintiff and Class Members were required to entrust their sensitive, non-public Private Information to one or more Defendants.

7. Vitruvian Health and NRS could not perform their regular business activities or generate revenue without collecting and maintaining Plaintiff's and Class Members' Private Information. Upon information and belief, Defendants retain the Private Information they collect for many years, even after their relationships with Plaintiff and Class Members end.

---

individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." *Id.*

[2] The Federal Trade Commission ("FTC") defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth. . . .." 17 C.F.R. § 248.201(b)(8).

[3] *See* Ex. 1.

8. Businesses that handle consumers' Private Information, like NRS, owe the individuals to whom the information relates a duty to adopt reasonable measures to protect it from disclosure and theft by unauthorized third parties, and to keep it safe and confidential. This duty arises under contract, statutory, and common law, industry standards, representations made to Plaintiff 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.

9. Similarly, healthcare entities that collect consumers' Private Information—such as Vitruvian Health—and provide this information to vendors and/or independent contractors like NRS—owe the individuals to whom the information relates a duty to ensure that the vendor and/or independent contractor utilizes and adopts reasonable measures 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 Plaintiff 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, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to NRS, and thus, NRS knew that failing to take reasonable steps to secure the Private Information left it in a dangerous condition.

11. Similarly, the possibility of a cyberattack and the potential for improper disclosure of Plaintiff's and Class Members' Private Information if inadequate data security was used by a vendor and/or independent contractor was a known risk to Vitruvian Health. Thus, Vitruvian Health knew that if it failed to select a vendor and/or independent contractor with adequate data

security that Plaintiff's and the Class's the Private Information would be left in a dangerous and vulnerable condition.

12. The Data Breach, which NRS failed to detect until cybercriminals had already **stolen** Plaintiff's and Class Members' Private Information, is the direct result of NRS's failure to implement basic data security measures or oversight over consumers' data in its custody and control. Had NRS implemented reasonable cybersecurity measures—including adequate safeguards for initial access, encryption, or redaction of personal data elements, and sufficient logging, monitoring, and alerting tools to detect unauthorized activity—criminals would not have been able to hack into NRS's servers, perform reconnaissance necessary to locate Plaintiff's and Class Members' Private Information, and then exfiltrate that data before being detected.

13. Furthermore, had Vitruvian Health ensured NRS implemented reasonable cybersecurity measures **prior** to utilizing NRS's services—including adequate safeguards for initial access, encryption or redaction of personal data elements, and sufficient logging, monitoring, and alerting tools to detect unauthorized activity—Plaintiff and Class Members would not have suffered the harm alleged herein.

14. NRS failed to adequately protect Plaintiff's and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive data when it was maintained on NRS's internet-accessible network without adequate safeguards against unauthorized access and exfiltration. This unencrypted, unredacted Private Information was compromised due to NRS's negligent acts and omissions and utter failure to protect it.

15. Similarly, Vitruvian Health failed to adequately protect Plaintiff's and Class Members' Private Information by failing to ensure the vendors and/or independent contractors it utilized, such as NRS, implemented industry standard data security procedures, practices, and

protocols to protect Plaintiff's and Class Members Private Information from hackers.

16. NRS breached its duties and obligations by failing in one or more of the following ways: (a) to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (b) to design, implement, and maintain reasonable data retention policies; (c) to adequately train or oversee its employees regarding data security; (d) to comply with industry standard data security practices; (e) to warn Plaintiff and Class Members and/or their agents of NRS's inadequate data security practices; (f) to encrypt or adequately encrypt the Private Information that was stored on NRS's network server; (g) to recognize or detect that its network systems repository had been compromised and accessed, or the extent of information compromised, in a timely manner to mitigate the harm; (h) to utilize widely available software able to detect and prevent this type of attack; and (i) to otherwise adequately secure the Private Information using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

17. Vitruvian Health breached its duties and obligations by: (a) failing to ensure NRS designed, implemented, monitored, and maintained reasonable network safeguards against foreseeable threats; (b) failing to ensure NRS designed, implemented, and maintained reasonable data retention policies; (c) failing to ensure NRS adequately trained or oversaw its employees regarding data security; (d) failing to ensure NRS complied with industry standard data security practices; (e) failing to warn Plaintiff and Class Members of NRS's inadequate data security practices; (f) failing to ensure NRS encrypted or adequately encrypted the Private Information that was stored on NRS's network server; (g) failing to ensure NRS had systems or processes in place to recognize or detect that NRS's network had been compromised and accessed; (h) failing to ensure NRS utilized widely available software able to detect and prevent this type of attack; and

(i) failing to ensure NRS otherwise adequately secured the Private Information of Plaintiff and the Class using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

18. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality and security of their Private Information. In providing their Private Information to one or more Defendants, Plaintiff and Class Members reasonably expected Defendants would keep their Private Information confidential and secure, use this information for only legitimate business purposes, and disclose it only as authorized. Defendants failed to do so, resulting in the unauthorized disclosure of Plaintiff's and Class Members' Private Information in the Data Breach.

19. Hackers targeted and obtained Plaintiff's and Class Members' Private Information from NRS because of the data's value in exploiting and stealing Plaintiff's and Class Members' identities. As a direct and proximate result of NRS's inadequate data security and breaches of its duties to handle Private Information with reasonable care, Plaintiff's and Class Members' Private Information was **accessed and acquired** by cybercriminals and exposed to an untold number of unauthorized individuals. The present and continuing risk to Plaintiff and Class Members as victims of the Data Breach will remain for their respective lifetimes.

20. The harm resulting from a cyberattack like this Data Breach manifests in numerous ways including identity theft and financial fraud. The exposure of an individual's Private Information due to a data breach ensures that the individual will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of his or her life. Mitigating that risk, to the extent even possible, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take several additional prophylactic measures. Plaintiff and Class Members will be

forced to allocate time to these tasks for years, if not their lifetimes, due to the Data Breach.

21. To make matters worse, although NRS confirmed the Data Breach's occurrence by July 11, 2024, Defendants waited **months** before beginning to notify Plaintiff and Class Members their Private Information had been compromised.

22. Further, upon information and belief, not all entities impacted by NRS's Data Breach have issued direct notice of the Data Breach to the victims. Thus, the full scope of the Data Breach is still unknown.

23. Defendants' delayed and vague reporting caused Plaintiff and Class Members to incur additional damages by diminishing their ability to timely and thoroughly address harms from the Data Breach, like by monitoring their account statements and obtaining identity theft protection services in the Data Breach's aftermath.

24. As a result of the Data Breach, Plaintiff and Class Members suffered concrete injuries in fact including, but not limited to (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) actual identity theft and fraud; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their Private Information; (g) loss of privacy; (h) emotional distress including anxiety and stress in with dealing with the Data Breach; and (i) the continued risk to their sensitive Private Information, which remains in Defendants' possession and is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect the PII they collect and maintain.

25. To recover for these harms, Plaintiff, on behalf of themselves and the Class as defined herein, bring claims for negligence/negligence *per se*, breach of implied contract, breach

of third-party beneficiary contract, unjust enrichment, declaratory/injunctive relief, and negligent hiring and supervision.

26. Plaintiff and Class Members seek compensatory, nominal, statutory, and punitive damages, declaratory judgment, and injunctive relief requiring NRS to (a) disclose, expeditiously, the full nature of the Data Breach and the types of Private Information exposed; (b) implement improved data security practices to reasonably guard against future breaches of Private Information; and (c) provide, at Defendants' own expense, all impacted Data Breach victims with lifetime identity theft protection services.

II. PARTIES

Plaintiff

27. Plaintiff **Gary Self** is a citizen and resident of Tunnel Hill, Georgia. Plaintiff Self received medical care from Vitruvian Health. Plaintiff Self received a Notice of Data Breach Letter from Vitruvian Health dated April 14, 2025, notifying him that his name, address, Social Security number, date of birth, financial account information, and other medical information were within the files stolen in the Data Breach.[4]

28. Plaintiff and the Class are current or former patients or customers, of companies that contracted NRS for services prior to July 5, 2024; thus, Plaintiff and the Class were and are NRS's ultimate customers. As a condition of and in exchange for their receipt of NRS's services, each Plaintiff was required to and did provide his or her Private Information to NRS.

Defendants

29. Defendant **Nationwide Recovery Service, Inc.** is a Tennessee corporation with a principal place of business at 545 West Inman Street, Cleveland, TN 37311. NRS may be served

[4] *See* Ex. 1.

by serving its registered agent Cogency Global, Inc. at 992 Davidson Dr., Ste. B, Nashville, TN 37205-1051.

30. Defendant **Hamilton Health Care System, Inc. d/b/a Vitruvian Health** is a Georgia non-profit corporation with its principal place of business located at 1200 Memorial Drive, Dalton Georgia, 30722-1900. Vitruvian Health may be served by serving its registered agent Savannah B. Moore at 1200 Memorial Dr., Dalton, GA 30720

III. JURISDICTION AND VENUE

31. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different than Defendants.

32. This Court has personal jurisdiction over NRS because it is headquartered in Tennessee. NRS regularly conducts business in Tennessee and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from Tennessee.

33. This Court has personal jurisdiction over Vitruvian Health because it regularly conducts business in Tennessee and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from Tennessee.

34. Defendants have purposely availed themselves of the rights and benefits of the state of Tennessee by engaging in activities including (a) directly and/or through their affiliates and agents providing services in this District; (b) conducting substantial business in this District; (c) having a registered agent to accept service of process in the state of Tennessee; and/or (d) engaging in other persistent courses of conduct and/or deriving revenue from services provided in Tennessee and in this District.

35. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendants reside within this District and/or have purposefully engaged in activities, including transacting business, in this District. Venue is also proper in this District pursuant to 28 U.S.C. § 1391(b)(2) as a substantial part of the events and/or omissions giving rise to the claims herein emanated from within this District, including the Data Breach at issue.

IV. GENERAL FACTUAL ALLEGATIONS

A. Defendants Collect and Maintain Private Information as Part of their Business for Profit.

36. NRS is a debt collection agency that provides services to entities such as Vitruvian Health.[5]

37. NRS has an estimated annual revenue of approximately $13.5 million.[6] In other words, NRS could have afforded to implement adequate data security but deliberately chose not to.

38. NRS recognized it had a duty to protect Private Information and states the following on its website: "[w]e respect your privacy and are committed to protecting it through our compliance with this policy."[7]

39. NRS's customers, such as Vitruvian Health, contract NRS to provide debt collection services.

40. In other words, NRS's business is collecting and maintaining consumers' data, including Plaintiff's and Class Members' Private Information.

[5] Ex. 1.
[6] https://www.zoominfo.com/c/nationwide-recovery-service-inc/82297975.
[7] https://nrsagency.com/privacy-policy/.

41. Considering NRS's business is collecting and maintaining Private Information, Vitruvian Health should have taken special care in selecting NRS to ensure it had adequate data security protocols in place to protect Private Information.

42. NRS derived economic benefits from collecting and using Plaintiff's and Class Members' Private Information.

43. Without the required submission of Private Information, NRS could not perform its operations, furnish the services it provides, or receive payment for those services.

44. As a condition of and in exchange for receiving services, Plaintiff and Class Members were required to entrust their highly sensitive Private Information to Vitruvian Health.

45. The data Defendants collect and maintain in the ordinary course of business includes full names, dates of birth, Social Security numbers, health information, and other sensitive data.

46. At all relevant times, NRS knew it was storing and using its network to store and transmit valuable, sensitive Private Information and that as a result, its systems would be attractive targets for cybercriminals.

47. NRS also knew that any breach of its information technology network and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the thousands of individuals whose Private Information was compromised, as well as intrusion into their private and sensitive personal matters.

48. In exchange for receiving Plaintiff's and Class Members' Private Information, NRS promised to safeguard the sensitive and confidential data, to use it only for authorized and legitimate purposes, and to delete such information from its systems once there was no longer a need to maintain it.

49. Upon information and belief, Vitruvian Health made promises and representations that the Private Information collected from them as a condition of obtaining services from Vitruvian Health, directly and indirectly, would be kept safe and confidential, so that the information's privacy would be maintained.

50. Based on the foregoing representations and warranties, and to obtain services from Vitruvian Health, Plaintiff and Class Members provided their Private Information to Vitruvian Health with the reasonable expectation and mutual understanding that Vitruvian Health would utilize vendors that would comply with its obligations to keep such information confidential and protected. Consumers, in general, demand security for their Private Information, especially when Social Security numbers and health data are involved.

51. The data NRS held in its network systems at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

B. NRS Owed Duties to Adopt Reasonable Data Security Measures for Private Information it Collected and Maintained.

52. As part of its business, NRS collects thousands of individuals' Private Information, including that of Plaintiff and Class Members, storing the data in its network server(s).

53. NRS had and continues to have duties to adopt reasonable measures to keep Plaintiff's and Class Members' Private Information confidential and protected from disclosure to unauthorized third parties, and to audit, monitor, and verify the integrity of its network server(s) where Private Information is stored.

54. NRS had and has obligations stemming from the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45, the Health Insurance Portability and Accountability Act ("HIPAA"), common law, contract, and industry standards, to keep Plaintiff's and Class Members' Private Information confidential and protected from unauthorized disclosure.

55. Additionally, by obtaining, using, and benefitting from Plaintiff's and Class Members' Private Information NRS assumed legal and equitable duties and knew or should have known it was responsible for protecting that Private Information from unauthorized access and disclosure.

56. NRS also owed a duty to protect Plaintiff and Class Members from the harm that insufficient data security and consequential exposure of their Private Information would cause, because such harm was foreseeable and reasonably preventable.

57. NRS knew it was storing valuable, sensitive Private Information in its network server(s) and that as a result, those systems would be an attractive target for cybercriminals.

58. NRS also knew that any breach of its systems and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the thousands of individuals whose Private Information was compromised, as well as intrusion into their private and sensitive personal financial and health matters.

59. NRS's duty to protect Plaintiff and Class Members from the foreseeable risk of injury that inadequate data protection and unauthorized exposure of their Private Information obligated NRS to implement reasonable practices to keep Plaintiff's and Class Members' sensitive Private Information confidential and securely maintained through reasonable, industry-standard, and legally compliant measures.

60. Additionally, upon information and belief, all contracts NRS entered into with its customers require NRS to implement and maintain reasonable, adequate, and legally compliant cybersecurity measures to protect its clients' Private Information against unauthorized disclosure and exfiltration.

61. Plaintiff and Class Members provided their Private Information to NRS pursuant to its agreements with its customers, were and are the intended beneficiaries of NRS's contractual obligation of reasonable, industry standard, and legally compliant data security for its clients' employees Private Information.

62. NRS's contractual obligations to safeguard Plaintiff's and Class Members' Private Information are an additional source of NRS's duty to protect Plaintiff's and Class Members' Private Information in its custody and control.

63. NRS owed the foregoing duties to protect Private Information maintained on its network systems from unauthorized disclosure and had the practical ability to fulfill those duties—yet failed to do so.

C. NRS Failed to Adequately Safeguard Plaintiff's and Class Member's Private Information, Resulting in a Massive and Preventable Data Breach.

64. On or about April 14, 2025, NRS began sending Plaintiff and other Data Breach victims correspondence regarding the Data Breach ("Notice Letters" or "Notice of Data Breach Letters").

65. The Notice Letters generally inform Plaintiff and Class Members as follows:

> We are writing to make you aware of an incident affecting your information. Nationwide Recovery Service ("NRS") is a third-party collection agency serving numerous clients across the U.S., including Hamilton Health Care System's affiliates Hamilton Emergency Medical Services, Hamilton Physician Group, Hamilton Medical Center, and Anna Shaw Children's Institute (collectively "Vitruvian Health"). NRS experienced a security incident affecting your information. Information systems maintained by Vitruvian Health were in no way affected by the security incident, which was limited to NRS systems.
>
> **What Happened**
>
> On July 11, 2024, NRS detected and began taking measures to address a cybersecurity incident affecting NRS systems. NRS started an investigation and implemented security measures to stop the unauthorized

access to NRS systems. The NRS investigation revealed that an unauthorized individual accessed NRS Systems from July 5, 2024 to July 11, 2024 and removed data from the system. Vitruvian Health was notified by NRS on February 24, 2025, that our patients' information was amongst the data affected by this incident. Since that time, Vitruvian Health has been working with NRS to confirm specific records affected so as to provide notification to those involved. Again, information systems maintained by Vitruvian Health were in no way affected by this security incident, which was limited to NRS systems.

What Information Was Involved

The affected NRS systems contained information of Vitruvian Health patients, including names, addresses, Social Security numbers, dates of birth, financial account information, and other medical information.

What We Are Doing

NRS has assured Vitruvian Health that NRS has implemented additional data security safeguards and reviewed its existing polices to improve its security posture to help prevent a similar incident form occurring in the future. Notifications have been provided to law enforcement and the credit monitoring bureaus. In addition, we are offering you identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We advise you to remain vigilant and periodically review your account information and credit reports for unauthorized activity. Additionally, we encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-877-434-0713, scanning the QR image, or going to https://response.idx.us/VitruvianHealth and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is July 14, 2025. We encourage you to take full advantage of this service offering. IDX representatives have been fully briefed on the incident and can answer questions or concerns you may have regarding protection of your personal information.[8]

[8] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/d271aa0a-908e-4430-bfe3-e9223d43cd21.html.

66. Omitted from the Notice Letters were the details of the root cause of the Data Breach, the identity of the perpetrator of the Data Breach, the vulnerabilities exploited, when the Data Breach began and ended, and the remedial measures undertaken to ensure such a data breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

67. Upon information and belief, had NRS implemented standard and reasonable digital forensic measures such as timestamping, intrusion detection systems, and logging aspects, it would be prepared for a forensic investigation of compromised information and would not need months to identify the information involved in the Data Breach. These failures exacerbated Plaintiff's and Class Members' damages, including actual damages in the form of lost opportunity costs, among others, by delaying and obfuscating NRS's notice of the Data Breach and depriving Plaintiff and Class Members of crucial time to mitigate and address it in a timely manner, like by putting credit freezes on their accounts or obtaining identity theft protection services.

68. Thus, NRS's purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiff and Class Members of the Data Breach's critical facts, like the status of NRS's investigation or the nature of the Private Information involved, with any degree of specificity or uniformity. Without these details, Plaintiff,' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

69. To make matters worse, NRS waited months after the Data Breach occurred to begin notifying Plaintiff and Class Members that the sensitive Private Information they entrusted to NRS is now in criminal hackers' possession. This unreasonable and unexplained delay deprived Plaintiff and Class Members of crucial time to address and mitigate the heightened risk of identity

theft and other harms resulting from the Data Breach.

70. NRS's insufficient data security for Plaintiff's and the Class's data caused and allowed criminals to target and take files containing Plaintiff's and Class Members' inadequately protected, unencrypted Private Information from NRS's network server, and unreasonably delayed Plaintiff's and Class Members' notice by months.

71. As the Data Breach and its timeline evidences, NRS did not use reasonable data security measures appropriate to the nature of the sensitive Private Information collected from Plaintiff and Class Members and maintained on NRS's network server(s), such as encrypting the information, deleting the data from NRS's server when it was no longer needed, requiring sufficient verification such as multi-factor authentication for accounts with access servers storing Private Information, training employees about cybersecurity and attempts to gain unauthorized access, investigating and addressing vulnerabilities in its data security practices, and/or implementing the necessary safeguards to enable NRS to identify malicious activity and curtail it when it happens. These failures allowed and caused cybercriminals to target NRS's network systems and carry out the Data Breach.

72. NRS could and should have prevented this Data Breach by ensuring its files and servers containing Plaintiff's and Class Members' Private Information were properly secured, sanitized, and encrypted and by using appropriate clearinghouse practices to purge consumer data that it was no longer required to maintain, but failed to do so.

73. NRS could and should have properly monitored its network for unauthorized access and unusual activity, including the downloading of large amounts of sensitive personal information from its network.

74. Additionally, NRS could have prevented the Data Breach by examining, testing,

and updating its cybersecurity practices to ensure vulnerabilities were identified and addressed and reasonable safeguards were continuously maintained, but failed to do so.

75. NRS could and should have implemented the following measures to prevent and detect the Data Breach, as recommended by the Microsoft Threat Protection Intelligence Team, but failed to do so:

> **Secure internet-facing assets**
>
> - Apply latest security updates
> - Use threat and vulnerability management
> - Perform regular audit; remove privileged credentials;
>
> **Include IT Pros in security discussions**
>
> - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely
>
> **Build credential hygiene**
>
> - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;
>
> **Apply principle of least-privilege**
>
> - Monitor for adversarial activities
> - Hunt for brute force attempts
> - Monitor for cleanup of Event Logs
> - Analyze logon events.[9]

76. NRS's tortious conduct and breach of contractual obligations, as detailed in herein, are evidenced by its failure to identify the scope of information involved and/or individuals impacted by the Data Breach until months after cybercriminals breached its network and accessed Plaintiff's and Class Members' Private Information stored therein—meaning NRS had no effective means in place to ensure that cyberattacks were detected, prevented, or timely investigated.

---

[9] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT THREAT INTELLIGENCE, (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster.

77. NRS's negligence in safeguarding Plaintiff's and Class Members' Private Information is exacerbated by the repeated warnings and alerts regarding the need to protect and secure sensitive data.

D. Vitruvian Health Negligently Utilized NRS's Services.

78. Vitruvian Health was negligent and failed to confirm when retaining NRS's services that Plaintiff's and Class Members' Private Information would be protected from unauthorized access, that NRS maintained adequate data security procedures, practices, infrastructure, and protocols, and that Plaintiff's and the Class's Private Information would not be subject to unauthorized access and exfiltration.

79. Vitruvian Health owed, and continues to owe, duties of care to Plaintiff and Class Members to: (a) exercise reasonable care to secure and protect the Private Information in its possession and the Private Information in the possession of any entity it hired to provide services—such as NRS—from unauthorized access; (b) ensure NRS implements adequate data security practices, procedures, infrastructure, and protocols compliant with applicable law and industry standards; (c) ensure NRS has adequate processes in place to quickly detect a data breach and to timely act on warnings regarding data breaches; (d) investigate NRS's data security practices, infrastructure, procedures, and protocols **prior** to retaining NRS; and (e) monitor NRS's security procedures, practices, and protocols during the entirety of the relationship.

80. Vitruvian Health utterly failed to uphold these duties, as evidenced by the Data Breach, thereby breaching its duties owed to Plaintiff and the Class.

81. As a direct and proximate cause of the Vitruvian Health's breaches, and failure to properly interview and vet NRS, Plaintiff and the Class have been damaged as set forth herein.

E. Defendants Knew of the Risk of a Cyberattack because Businesses in Possession of Private Information are Particularly Susceptible to Breaches.

82. Defendants' negligence, including their gross negligence in failing to safeguard Plaintiff's and Class Members' Private Information, is exacerbated by the repeated warnings and alerts directed to protect and secure sensitive data.

83. Private Information—including the types accessed in the Data Breach—are of great value to cybercriminals because this information can be used for a variety of unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the internet black market known as the dark web.

84. Private Information can also be used to distinguish, identify, or trace an individual's identity, such as his or her name, Social Security number, and financial records. This may be accomplished alone, or in combination with other personal or identifying information connected or linked to an individual such as his or her birthdate, birthplace, and mother's maiden name.

85. Data thieves regularly target entities that store Private Information like NRS due to the highly sensitive information they maintain. NRS knew and understood that Plaintiff's and Class Members' Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize it through unauthorized access.

86. Cyberattacks against institutions like NRS are targeted and frequent. According to Contrast Security's 2023 report, "Cyber Bank Heists: Threats to the financial sector," "[o]ver the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[10]

[10] Tom Kellermann, *Cyber Bank Heists: Threats to the financial sector*, at 5, CONTRAST SECURITY, available at: https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%202023.pdf?hsLang=en.

87. According to the Identity Theft Resource Center's report covering the year 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[11] As stated in IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[12]

88. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in NRS's industry, including NRS itself.

89. NRS's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches targeting entities like NRS that collect and store Private Information preceding the date of the subject Data Breach.

90. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims. The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points. The 2023 compromises represent a 78-percentage point increase over the previous year and a 72-percentage point hike from the previous all-time high number of compromises (1,862) set in 2021.

---

[11] *See 2021 Annual Data Breach Report Sets New Record for Number of Compromises*, ITRC (Jan. 24, 2022), available at: https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises.

[12] *Cost of a data breach 2022: A million-dollar race to detect and respond*, IBM, available at: https://www.ibm.com/reports/data-breach.

91. Additionally, as companies became more dependent on computer systems to run their business,[13] e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[14]

92. Entities with custody of PHI, like NRS, reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.[15] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage. Almost 50% of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[16]

---

[13] *FEDS Notes*, *Implications of Cyber Risk for Financial Stability*, BD. GOVERNORS OF THE FED. RES. SYS., (May 12, 2022), https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited April 1, 2025).

[14] Suleyman Ozarslan, *Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022*, PICUS, (Mar. 24, 2022), https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last visited April 1, 2025).

[15] *See 2022 Annual Data Breach Report*, ITRC, available at: https://www.idtheftcenter.org/publication/2022-data-breach-report.

[16] *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 (last visited April 1, 2025).

93. Thus, the healthcare industry, and business operating within and aiding the healthcare industry, have become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[17]

94. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

95. 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 patient'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."[18] A complete identity theft kit with health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[19]

96. NRS knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for it.

97. NRS was clearly aware of the risks it was taking and the harm that could result from inadequate data security but threw caution to the wind.

---

[18] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDEXPERTS (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited April 1, 2025).

[19] *Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS, (Sept. 30, 2014), available at: https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

98. Similarly, Vitruvian Health knew the importance of selecting a vendor and/or independent contractor with adequate data security given the well-publicized rise in data breaches but failed to ensure NRS deployed adequate data security.

99. As a business in possession of customers' Private Information, NRS knew, or should have known, the importance of safeguarding the Private Information entrusted to it, directly and indirectly, by Plaintiff and Class Members, and of the foreseeable consequences if its network systems were breached. Such consequences include the significant costs imposed on Plaintiff and Class Members due to their Private Information's disclosure to cybercriminals. Nevertheless, NRS failed to implement or follow reasonable cybersecurity measures to protect against the foreseeable harm of this Data Breach.

100. Additionally, as businesses in possession of customers' Private Information, like Vitruvian Health, knew or should have known, the importance of safeguarding the Private Information entrusted to it, directly and indirectly, and of the foreseeable consequences if it willingly gave Plaintiff's and the Class's Private Information to a vendor and/or independent contractor with inadequate data security. Such consequences include the significant costs imposed on Plaintiff and Class Members due to their Private Information's disclosure to cybercriminals.

101. NRS was, or should have been, fully aware of the unique type and the significant volume of data on its network server(s), amounting to thousands of individuals' detailed Private Information, and, thus, the wide extent of individuals who the exposure of that unencrypted data would harm.

102. Given the nature of the Data Breach, it was foreseeable that Plaintiff's and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals for use in variety of different injurious ways. Indeed, the cybercriminals who

possess Plaintiff's and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiff's and Class Members' names.

103. Plaintiff and Class Members were the foreseeable and probable victims of NRS's inadequate security practices and procedures. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, medical and financial fraud, and the like.

F. NRS was Required, But Failed, to Comply with FTC Rules and Guidance.

104. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

105. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which establishes cyber-security guidelines for businesses like NRS. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

106. The FTC's guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

107. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

108. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential data, treating 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 of the FTC Act. Orders resulting from these actions further clarify the measures business like NRS must undertake to meet their data security obligations.

109. Such FTC enforcement actions include actions against entities in the healthcare industry like NRS. *See, e.g.*, *In the Matter of LabMD, Inc.*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

110. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as NRS, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above are also a basis of NRS's duties in this regard.

111. The 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 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." NRS itself profits from collecting and managing Plaintiff's and Class Members' data.

112. NRS failed to properly implement basic data security practices, in violation of its duties under the FTC Act.

113. NRS's failure to employ reasonable and appropriate means to protect against unauthorized access to Plaintiff's and Class Members' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by the FTC Act.

G. NRS was Required, But Failed, to Comply with HIPAA.

114. NRS is a business associate, as defined under HIPAA (45 C.F.R. §§ 160.102, 160.103), and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160, Part 164, Subparts A and E; and Security Rule, 45 C.F.R. Part 160, Part 164, Subparts A, C, D, and E.

115. NRS is further subject to the Health Information Technology Act ("HITECH")'s rules for safeguarding electronic forms of medical information. *See* 42 U.S.C. §17921; 45 C.F.R. § 160.103.

116. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting PHI that is kept or transferred in electronic form.

117. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

118. HIPAA's Security Rule required and requires that NRS do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

119. HIPAA also required and requires NRS to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, NRS is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. §164.312(a)(1).

120. HIPAA and HITECH also require procedures to prevent, detect, contain, and correct data security violations and disclosures of PHI that are reasonably anticipated but not permitted by privacy rules. *See* 45 C.F.R. § 164.306(a)(1), (a)(3).

121. HIPAA further requires business associates like NRS to have and apply appropriate sanctions against members of their workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

122. Further, HIPAA requires business associates like NRS to mitigate, to the extent practicable, any harmful effect that is known to the entity of a use or disclosure of PHI in violation of the entity's policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the business associate. *See* 45 C.F.R. § 164.530(f).

123. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule."[20] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology, which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI."[21]

124. HIPAA's Breach Notification Rule further requires that within 60 days of discovering a breach of unsecured PHI. NRS must notify each individual affected regarding the nature of the breach, the PHI compromised, steps the individual should take to protect against potential resulting harm, and what NRS is doing to protect against future breaches. 45 C.F.R. § 164.404(b).

125. HIPAA requires that when a covered entity, like Plaintiff's and Class Members' health plans serviced by NRS, *see* 45 C.F.R. § 160.103, provides PHI to a business associate, like

---

[20] *Security Rule Guidance Material*, HHS (Aug. 21, 2024), available at: https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

[21] *Guidance on Risk Analysis*, HHS (July 22, 2024), available at: https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es.

NRS, the covered entity must require by contract and ensure that the business associate uses appropriate safeguards to protect electronic PHI from unauthorized disclosure. 45 C.F.R. § 164.504(e)(2)(ii).

126. As alleged herein, NRS violated HIPAA and HITECH. Specifically, NRS (a) failed to maintain adequate security practices, systems, and protocols to prevent data loss, (b) failed to mitigate the risks of a data breach, (c) failed to ensure the confidentiality and protection of PHI, (d) failed to use appropriate safeguards to prevent the unauthorized disclosure of Plaintiff's and Class Members' Private Information, and (e) failed to provide the required Data Breach notice within 60 days of discovering the incident.

H. NRS Failed to Comply with Industry Standards.

127. A number of published industry and national best practices are widely used as a go-to resource when developing an institution's cybersecurity standards.

128. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.

129. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

130. Further still, CISA makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.

131. Upon information and belief, NRS failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST

Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiff's and Class Members' Private Information, resulting in the Data Breach.

132. Additionally, as explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[22]

133. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, NRS could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

[22] *See How to Protect Your Networks from RANSOMWARE*, at 3, FBI, available at: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

d. Configure firewalls to block access to known malicious IP addresses.

e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

f. Set anti-virus and anti-malware programs to conduct regular scans automatically.

g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

h. Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

k. Consider disabling Remote Desktop protocol (RDP) if it is not being used.

l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

m. Execute operating system environments or specific programs in a virtualized environment.

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[23]

134. Further, NRS could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

a. **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

b. **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

c. **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

d. **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

[23] *Id.* at 3–4.

e. **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

f. **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

g. **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[24]

135. Given that NRS was storing the Private Information of millions of individuals, it could have and should have implemented all the above measures to prevent and detect ransomware attacks.

136. Specifically, among other failures, NRS had far too much confidential unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.[25]

---

[24] *See Security Tip (ST19-001) Protecting Against Ransomware*, CISA (original release date Apr. 11, 2019), available at: https://www.cisa.gov/news-events/news/protecting-against-ransomware.

[25] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, FORTRA (Aug. 14, 2018), https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption (April 1, 2025).

137. NRS should have also limited remote access credentials for portions of its network on which Private Information was stored to ensure that stolen credentials cannot be used to access its entire network.

138. Moreover, it is a well-established industry standard practice for a business to dispose of confidential Private Information once it is no longer needed. The FTC, among others, has repeatedly emphasized the importance of disposing of unnecessary Private Information: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not on your system, it can't be stolen by hackers."[26] NRS, rather than following this basic standard of care, kept thousands of individuals' unencrypted Private Information indefinitely, years after the customer relationship ended.

139. In summary, the Data Breach could have readily been prevented using industry standard network segmentation and encryption of all Private Information.

140. The Data Breach could have also been readily prevented by: (a) using two-factor authentication; (b) regularly changing usernames and passwords and using strong usernames and passwords; (c) updating all software often and regularly; (d) using firewalls to restrict access; and (e) network level authentication for remote desktop connection.

141. Further, the scope of the Data Breach could have been dramatically reduced had NRS utilized proper record retention and destruction practices.

I. Defendants Owed Plaintiff and Class Members Common Law Duties to Safeguard their Private Information.

[26] *Protecting Private Information: A Guide for Business*, FTC, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf, at p. 6.

142. In addition to its obligations under federal and state laws, NRS owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. These duties owed to Plaintiff and Class Members obligated NRS to provide reasonable data security consistent with industry standards and requirements to protect Plaintiff's and Class Members' Private Information in its care from unauthorized disclosure, and to timely and adequately warn Plaintiff and Class Members in the event their Private Information was compromised.

143. Furthermore, Vitruvian Health owed a duty to Plaintiff and Class Members to exercise reasonable care in selecting a vendor and/or independent contractor such as NRS. Vitruvian Health should have ensured that any vendor and/or independent contractor it selected secured, safeguarded, protected, retained, and deleted, the Private Information in its possession to avoid it from being compromised, lost, stolen, accessed, and misused by unauthorized persons. These duties owed to Plaintiff and Class Members obligated Vitruvian Health to select a vendor and/or independent contractor with reasonable data security consistent with industry standards and requirements to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure, and to timely and adequately warn Plaintiff and Class Members in the event their Private Information was compromised.

144. NRS owed duties to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information on how to adequately protect the data.

145. Vitruvian Health owed duties to Plaintiff and Class Members to ensure any vendor and/or independent contractor hired created and implemented reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information on how to adequately protect the data

146. NRS owed duties to Plaintiff and Class Members to implement processes that would detect a compromise of Private Information in a timely manner, before thousands of individuals' Private Information was taken.

147. Vitruvian Health owed duties to Plaintiff and Class Members to ensure any vendor and/or independent contractor hired implemented processes that would detect a compromise of Private Information in a timely manner, before thousands of individuals' Private Information was taken.

148. NRS owed duties to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

149. Vitruvian Health owed duties to Plaintiff and Class Members to ensure any vendor and/or independent contractor hired acted upon data security warnings and alerts in a timely fashion

150. NRS owed duties to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred, and the extent of Private Information involved.

151. Vitruvian Health owed duties to Plaintiff and Class Members to ensure any vendor and/or independent contractor they utilized disclosed in a timely and accurate manner when and how the Data Breach occurred, and the extent of Private Information involved.

152. NRS owed duties to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

153. Vitruvian Health owed duties to Plaintiff and Class Members because they were foreseeable and probable victims of any vendors and/or independent contractors with inadequate data security practices.

154. NRS failed to take the necessary precautions to safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized disclosure. NRS's actions and omissions represent a flagrant disregard of Plaintiff's and Class Members' rights.

155. Vitruvian Health failed to take the necessary precautions to safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized disclosure. Vitruvian Health's actions and omissions represent a flagrant disregard of Plaintiff's and Class Members' rights.

J. Plaintiff and Class Members Suffered Common Injuries and Damages due to Defendants' Misconduct.

156. NRS's failure to implement or maintain adequate data security measures for Plaintiff's and Class Members' Private Information directly and proximately injured Plaintiff and Class Members by the resulting disclosure of their Private Information in the Data Breach.

157. Vitruvian Health's failure to ensure the vendor and/or independent contractor utilized implemented or maintained adequate data security measures for Plaintiff's and Class Members' Private Information directly and proximately injured Plaintiff and Class Members by the resulting disclosure of their Private Information in the Data Breach.

158. The ramifications of Defendants' failures to keep Plaintiff's and Class Members' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

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

160. Upon information and belief, Plaintiff and Class Members are also at a continued risk of harm because Vitruvian Health has not ceased using NRS's services. Plaintiff and Class Members are subject to further attack so long as Vitruvian Health negligently continues to use NRS's services.

161. As a result of NRS's ineffective and inadequate data security practices, the consequential Data Breach, and the foreseeable outcome of Plaintiff's and Class Members' Private Information ending up in criminals' possession, all Plaintiff and Class Members have suffered and will continue to suffer the following actual injuries and damages, without limitation: (a) invasion of privacy; (b) financial 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, and related lost opportunity costs; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their Private Information; (g) loss of the benefit of their bargain with NRS; (h) emotional distress including anxiety and stress in dealing with the Data Breach's aftermath; and (i) the continued risk to their sensitive Private Information, which remains in NRS's possession and is subject to further unauthorized disclosures so long as NRS fails to undertake appropriate and adequate measures to protect the Private Information it collects and maintains.

162. As a result of Vitruvian Health failing to ensure NRS implemented adequate data security practices—resulting in the consequential Data Breach—all Plaintiff and Class Members

have suffered and will continue to suffer the following actual injuries and damages, without limitation: (a) invasion of privacy; (b) financial 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, and related lost opportunity costs; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their Private Information; (g) loss of the benefit of their bargain; (h) emotional distress including anxiety and stress in dealing with the Data Breach's aftermath; and (i) the continued risk to their sensitive Private Information, which remains in NRS's possession and is subject to further unauthorized disclosures so long as Vitruvian Health continues to use NRS's services.

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

163. Plaintiff and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

164. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[27] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[28]

165. 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.

[27] 17 C.F.R. § 248.201 (2013).
[28] *Id.*

Criminals monetize the data by selling the stolen information on the internet black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

166. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[29] 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.[30] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

167. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, PHI and PII like the Private Information at issue here.[31] The digital character of Private Information 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 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,

---

[29] Louis DeNicola, *What Is the dark web?*, EXPERIAN (May 12, 2021), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited April 1, 2025).

[30] *Id.*

[31] *What is the dark web?*, MICROSOFT 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last visited April 1, 2025).

dates of birth, and medical information.[32] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[33]

168. The unencrypted Private Information of Plaintiff and Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted and detailed Private Information may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized actors can easily access and misuse Plaintiff's and Class Members' Private Information due to the Data Breach.

169. 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 to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

170. 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.

---

[32] *Id.*; Louis DeNicola, *What Is the dark web?*, EXPERIAN (May 12, 2021), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited April 1, 2025).

[33] *What is the dark web?*, MICROSOFT 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last visited April 1, 2025).

171. Another such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[34]

172. With "Fullz" packages, cybercriminals can cross-reference two (2) sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

173. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's 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 that was exfiltrated in the Data Breach, criminals may still 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.

174. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

---

[34] "Fullz" is fraudster speak for data that includes the victim's information, including but not limited to name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Recs. for Sale in Underground Stolen from Texas Life Ins. Firm*, KREBS ON SECURITY (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last visited April 1, 2025).

175. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

176. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that their stolen Private Information is being misused, and that such misuse is traceable to the Data Breach.

177. Social Security numbers, for example, are among the worst kind of personal information to have been 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, as is the case here, 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.[35]

178. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information

[35] *Identity Theft and Your Social Security Number*, Pub. No. 06-10064, SOCIAL SECURITY ADMIN. (June 2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

increases."[36] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[37]

179. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[38] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[39]

180. What is more, it is no 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.

181. 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."[40]

182. 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

---

[36] *See Avoid Identity Theft: Protect Social Security Numbers*, SOCIAL SECURITY ADMIN., https://www.ssa.gov/phila/ProtectingSSNs.htm (last visited April 1, 2025).
[37] *Id.*
[38] *See How to Protect Yourself from Social Security Number Identity Theft*, EQUIFAX https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft (last visited April 1, 2025).
[39] *See* Julia Kagan, *What is an SSN? What to Know About Social Security Numbers*, INVESTOPEDIA (Sept. 2, 2024), https://www.investopedia.com/terms/s/ssn.asp (last visited April 1, 2025).
[40] 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 (last visited April 1, 2025).

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 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 credit lines.[41]

183. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft.

184. Similarly, the California state government warns consumers: "Originally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[42]

185. Theft of PHI, in particular, is gravely serious as well: "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."[43]

---

[41] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMIN. (2018), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[42] *See Your Social Security Number: Controlling the Key to Identity Theft*, OFFICE OF THE ATTORNEY GENERAL OF CAL., https://oag.ca.gov/idtheft/facts/your-ssn (last visited April 1, 2025).

[43] *See What to Know About Medical Identity Theft*, FED. TRADE COMM'N, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited April 1, 2025).

186. PHI is likely to be used in detrimental ways, including by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[44]

187. Another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[45]

188. "Actors buying and selling PII and PHI 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."[46]

189. "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."[47]

190. 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."[48]

---

[44] *Id.*

[45] *70% Of Data Involved In Healthcare Breaches Increases Risk of Fraud*, DISTILINFO (Oct. 3, 2019), https://distilgovhealth.com/2019/10/03/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud (last visited April 1, 2025).

[46] *Id.*

[47] *The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches*, EXPERIAN, available at: https://stg1.experian.com/assets/data-breach/white-papers/experian-medical-id-theft-healthcare.pdf.

[48] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH (Oct. 30, 2019) https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited April 1, 2025).

191. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice,

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[49]

192. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[50]

193. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[51] Yet, NRS failed to rapidly report to Plaintiff and Class Members that their Private Information was stolen.

194. 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.

195. 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

---

[49] Erika Harrell, *Bureau of Just. Stat.*, NCJ 256085, U.S. DEP'T OF JUST., *Victims of Identity Theft*, 2018 I (2020), available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf.
[50] *See 2019 Internet Crime Report Released*, FBI (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited April 1, 2025).
[51] *Id.*

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.

196. 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, Plaintiff and Class Members will need to remain vigilant for years or even decades to come.

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

197. As a result of the recognized risk of identity theft, when a data breach occurs, 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 asset of time has been lost.

198. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face substantial costs and time to repair the damage to their good name and credit record.

199. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate that harm.

200. Plaintiff and Class Members have spent time, 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.

201. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps 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 seven 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.[52]

202. 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, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of NRS's conduct and failures that caused the Data Breach.

Diminished Value of Private Information.

203. Private Information is a valuable property right.[53] 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. Indeed, NRS itself profits from Plaintiff's and Class Members' data.

204. For example, drug and medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase Private Information on the black market for the

---

[52] *See What to do Right Away, FTC*, https://www.identitytheft.gov/Steps (last visited Apr. 1, 2025)

[53] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PRIVATE INFORMATION") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009) ("PRIVATE INFORMATION, 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).

purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongly disclosed PHI to adjust their insureds' medical insurance premiums.

205. Private Information can sell for as much as $363 per record according to the Infosec Institute.[54]

206. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data sells on the dark web for $50 and up.

207. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[55] In fact, the data marketplace is 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.[56] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[57]

208. As a result of the Data Breach, Plaintiff's, 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 likely release onto the dark web, where it holds significant value for the threat actors.

---

[54] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited April 1, 2025).

[55] David Lazarus, *Shadowy data brokers make the most of their invisibility cloak*, LA TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Apr. 1, 2025).

[56] DATACOUP, https://datacoup.com/ (last visited April 1, 2025).

[57] *Frequently Asked Questions*, NIELSEN, available at: https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

209. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

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

210. To date, Defendants have done little to nothing to provide Plaintiff and Class Members with relief for the damages they have suffered due to the Data Breach.

211. 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, filing false tax returns, taking out loans or lines of credit, or filing false unemployment claims.

212. 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 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.

213. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

breach, where victims can easily cancel or close credit and debit card accounts.[58] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers). Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future, if not forever.

214. 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 NRS's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for NRS's failure to safeguard their Private Information.

V. PLAINTIFF'S EXPERIENCES AND INJURIES

Plaintiff Self

215. Plaintiff Self received a Notice Letter from Vitruvian Health informing him that his highly confidential Private Information was compromised in the Data Breach.

216. Upon information and belief, NRS obtained Plaintiff Self's Private Information through Vitruvian Health.

217. Plaintiff Self greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Self diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

---

[58] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The dark web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last visited April 1, 2025).

218. At the time of the Data Breach NRS retained Plaintiff Self's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Self's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

219. As a result of the Data Breach, Plaintiff Self has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to investigating the Data Breach, investigating how best to ensure that he is protected from identity theft, and reviewing account statements, credit reports, and/or other information. Plaintiff Self estimates he has spent ***hours*** on these mitigation activities in response to the Data Breach—valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

220. Plaintiff Self further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

221. Due to the Data Breach, Plaintiff Self is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

222. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Self's and Class Members' Private Information was targeted, accessed, and stolen.

223. Plaintiff Self further believes his Private Information, and that of Class Members, was and will be sold and disseminated on the dark web following the Data Breach—if this has not happened already—as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

224. The Data Breach caused Plaintiff Self to suffer fear, anxiety, and stress, knowing that thieves intentionally targeted and stole his Private Information, including his Social Security number, and knowing that his Private Information is in the hands of cybercriminals.

VI. CLASS ACTION ALLEGATIONS

225. Plaintiff brings this nationwide class action on behalf of themselves, and all others similarly situated pursuant to Federal Rule of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

226. The Classes Plaintiff seek to represent are defined as follows ("Class"):

> **Nationwide Class:**
>
> All United States citizens whose Private Information was compromised in the Data Breach, including all persons who were sent a Notice Letter.

227. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

228. Plaintiff reserves the right to amend the definition of the Class or add a Class or Subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

229. Numerosity. The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiff and exclusively in the possession of NRS.

230. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

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

b. Whether NRS had the duty not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether NRS had the duty not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to safeguard the Private Information of Plaintiff and Class Members;

e. Whether and when NRS actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendants violated the law by failing to timely notify Plaintiff and Class Members that their Private Information had been compromised;

h. Whether NRS failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Vitruvian Health failed to ensure NRS implemented and maintained reasonable data security procedures and practices to prevent the Data Breach;

j. Whether NRS adequately addressed and fixed the vulnerabilities that permitted the Data Breach to occur;

k. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct; and,

l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

231. Typicality. Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, were exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

232. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the Class, 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 Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

233. Adequacy. Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff have retained counsel experienced in complex class action and data breach litigation, and Plaintiff intend to prosecute this action vigorously.

234. Superiority and Manageability. 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 Defendants. Further, 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.

235. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they 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 Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

236. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

237. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

238. Unless a Class-wide injunction is issued, Defendants may continue to inadequately protect and secure the Private Information of Class Members, may continue to refuse to provide

proper notification to Class Members regarding the Data Breach, and may continue to act unlawfully as set forth in this Complaint.

239. Further, Defendants acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

240. Likewise, particular issues under Rule 23(c)(2) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the Plaintiff and the class of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information and selecting vendors and/or independent contractors;

c. Whether NRS's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether NRS's failure to institute adequate protective security measures amounted to negligence;

e. Whether NRS failed to take commercially reasonable steps to safeguard their customers' Private Information; and,

f. Whether adherence to FTC and/or HIPAA data security rules, and measures recommended by data security experts would have reasonably prevented the Data Breach.

VII. CAUSES OF ACTION

COUNT I
NEGLIGENCE/NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Nationwide Class against NRS)

241. Plaintiff re-alleges and incorporates by reference paragraphs 1–240 above as if fully set forth herein.

242. NRS solicited, accepted, and stored the Private Information of Plaintiff and the Class.

243. The Private Information included Plaintiff's and Class Members' names, dates of birth, Social Security numbers, and health information.

244. NRS had full knowledge of the sensitivity of the Private Information to which it was entrusted, and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed to unauthorized persons.

245. NRS had duties to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting their Private Information.

246. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices by NRS.

247. Plaintiff and Class Members had no ability to protect their Private Information in NRS' possession.

248. By collecting and storing Plaintiff's and Class Members' Private Information, NRS had a duty of care to use reasonable means to secure and safeguard it, to prevent disclosure of the information, and to safeguard the Private Information from theft.

249. NRS's duty of care obligated it to implement processes by which it could detect if Private Information was exposed to unauthorized actors and have processes in place through which it could detect if Private Information was exposed to unauthorized actors.

250. NRS owed a duty to Plaintiff and Class Members to: (a) provide data security consistent with industry standards and legal and regulatory requirements; and (b) ensure that its systems and networks and the personnel responsible for them adequately protected Plaintiff's and Class Members' Private Information.

251. NRS had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

252. Pursuant to the FTC Act, NRS had a duty to provide adequate systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

253. Pursuant to HIPAA, 42 U.S.C. § 1302d *et seq*., NRS had the further duty to implement reasonable safeguards to protect Plaintiff's and Class Members' PHI from unauthorized disclosure.

254. Pursuant to HIPAA, NRS had a duty to implement reasonable data security measures for the PHI in its care, including by, *e.g.*, rendering the electronic PHI it maintained in a form unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* 45 C.F.R. § 164.304.

255. Additionally, pursuant to HIPAA, NRS had a duty to provide notice of the Data Breach within 60 days of discovering it. *See* 42 C.F.R. § 2.16(b); 45 C.F.R. § 164.404(b).

256. NRS breached its duties to Plaintiff and Class Members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information, by failing to encrypt or timely delete the Private Information from its network systems, and by failing to timely or adequately notify or warn Plaintiff and Class Members about the Data Breach.

257. NRS's violations of the FTC Act and HIPAA as described herein directly caused and/or were a substantial factor in the Data Breach and resulting injuries to Plaintiff and Class Members.

258. Plaintiff and Class Members are within the class of persons the FTC Act and HIPAA were intended to protect.

259. The type of harm that resulted from the Data Breach was the type of harm the FTC Act and HIPAA were intended to guard against.

260. NRS's failure to comply with the FTC Act and HIPAA is negligence *per se.*

261. NRS's duties to use reasonable care in protecting Plaintiff's and Class Members' Private Information arose not only as a result of the statutes and regulations described above, but because NRS are bound by industry standards to secure such Private Information.

262. NRS breached its duties and was negligent by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure in the Data Breach. The specific negligent acts and omissions committed by NRS include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

b. Failing to adequately train employees on proper cybersecurity protocols;

c. Failing to adequately monitor the security of its information technology networks and systems;

d. Failure to periodically ensure that its network systems had plans in place to maintain reasonable data security safeguards;

e. Allowing unauthorized access to Plaintiff's and Class Members' Private Information; and

f. Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

263. But for NRS's wrongful and negligent breaches of its duties owed to Plaintiff and Class Members, the Data Breach would not have occurred or at least would have been mitigated, Plaintiff's and Class Members' Private Information would not have been compromised, and Plaintiff's and Class Members' injuries would have been avoided.

264. It was foreseeable that NRS's failures to use reasonable measures to protect Plaintiff's and Class Members' Private Information would injure Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable to NRS given the known high frequency of cyber-attacks and data breaches in NRS's industry.

265. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would cause them one or more types of injuries.

266. As a direct and proximate result of NRS's negligence, Plaintiff and Class Members have suffered and will suffer injuries and damages, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) actual identity theft and fraud; (d) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (e) loss of benefit of their bargain; and (f) the continued and certainly increased risk to their Private Information, which remains (i) unencrypted and available for unauthorized third parties to access and abuse; and (ii) in NRS's possession and subject to further unauthorized disclosures so long as NRS fails to undertake appropriate and adequate measures to protect it.

267. As a direct and proximate result of NRS's negligence, Plaintiff and Class Members have suffered and will continue to suffer injuries and/or harm, including but not limited to anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

268. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class against all Defendant Vitruvian Health)

269. Plaintiff re-alleges and incorporates by reference paragraphs 1–240 above as if fully set forth herein, and bring this claim against all Vitruvian Health.

270. Vitruvian Health required Plaintiff and Class Members to provide and entrust their Private Information to Vitruvian Health as a condition of obtaining services, benefits, and/or employment.

271. When Plaintiff and Class Members provided their Private Information to Vitruvian Health, they entered into implied contracts with Vitruvian Health. Pursuant to these contracts,

Vitruvian Health agreed, as manifested through their conduct, to safeguard and protect such Private Information and to timely and accurately notify Plaintiff and Class Members if and when their Private Information was breached and compromised.

272. Specifically, Plaintiff and Class Members entered into valid and enforceable implied contracts with Vitruvian Health when they agreed to provide their Private Information and/or payment to Vitruvian Health, and Vitruvian Health agreed to collect, maintain, and profit from that Private Information.

273. The valid and enforceable implied contracts that Plaintiff and Class Members entered into with Vitruvian Health included Vitruvian Health' promises to protect Private Information it collected from Plaintiff and Class Members against unauthorized disclosures. Plaintiff and Class Members provided this Private Information in reliance on Vitruvian Health' promises.

274. Under the implied contracts, Vitruvian Health promised and was obligated to protect Plaintiff's and Class Members' Private Information. In exchange, Plaintiff and Class Members agreed to provide Vitruvian Health with their Private Information.

275. Vitruvian Health promised and warranted to Plaintiff and Class Members, through privacy documents and conduct, to maintain the privacy and confidentiality of the Private Information they collected from Plaintiff and Class Members and to keep such information safeguarded against unauthorized access and disclosure.

276. Vitruvian Health' adequate protection of Plaintiff's and Class Members' Private Information was a material aspect of these implied contracts with Vitruvian Health.

277. Vitruvian Health solicited and invited Plaintiff and Class Members to provide their Private Information as part of Vitruvian Health' regular business practices. Plaintiff and Class

Members accepted Vitruvian Health' offers and provided their Private Information to Vitruvian Health.

278. By entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Vitruvian Health would ensure any vendors and/or independent contractors Vitruvian Health selected and utilized complied with industry standards and relevant laws and regulations, including the FTC Act, HIPAA, and HITECH.

279. Plaintiff also reasonably believed that Vitruvian Health would properly vet and inquire into the data security of any vendor and/or independent contractor it used—such as NRS—to ensure their Private Information was adequately protected and not susceptible to data breaches.

280. Plaintiff and Class Members, who contracted with Vitruvian Health, provided their Private Information to Vitruvian Health and reasonably believed and expected that (Vitruvian Health would utilize vendors and/or independent contractors with adequate data security to protect their Private Information. However, Vitruvian Health utterly failed to do so.

281. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their Private Information to Vitruvian Health and agreed Vitruvian Health would receive payment for and benefit from, amongst other things, the protection of their Private Information.

282. Plaintiff and Class Members performed their obligations under the contracts when they provided their Private Information and/or payment to Vitruvian Health.

283. Vitruvian Health materially breached their contractual obligations to protect the Private Information they required Plaintiff and Class Members to provide when that Private Information was unauthorizedly disclosed in the Data Breach due to: (a) NRS's inadequate data security measures and procedures; and (b) Vitruvian Health's failure to ensure its vendors and/or

independent contractors—such as NRS—had adequate data security measures and procedures in place.

284. Vitruvian Health materially breached their contractual obligations to deal in good faith with Plaintiff and Class Members when: (a) NRS failed to take adequate precautions to prevent the Data Breach; (b) Vitruvian Health failed to ensure NRS took adequate precautions to prevent a data breach; and (c) Vitruvian Health failed to timely or adequately notify Plaintiff and Class Members about the Data Breach.

285. The Data Breach was a reasonably foreseeable consequence of Vitruvian Health' conduct, by acts of omission or commission, in breach of these implied contracts with Plaintiff and Class Members.

286. As a result of NRS's failure to fulfill the data security protections promised in these contracts and Vitruvian Health's failure to utilize vendors and/or contractors with adequate data security protections, Plaintiff and Class Members did not receive the full benefit of their bargains with Vitruvian Health and instead received services of a diminished value compared to that described in the implied contracts. Plaintiff and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they were promised and that which they received.

287. Had Vitruvian Health disclosed that it would be using a vendor and/or independent contractor with inadequate data security or that it would not be vetting potential vendors and/or independent contractors to ensure they had adequate data security Plaintiff, and the Class would not have contracted with Vitruvian Health.

288. Plaintiff and Class Members would not have provided and entrusted their Private Information to Vitruvian Health in the absence of the implied contracts between them and Vitruvian Health.

289. Plaintiff and Class Members fully performed their obligations under their implied contracts with Vitruvian Health.

290. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or restitution damages, in an amount to be proven at trial, due to Vitruvian Health's breach of implied contract.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Nationwide Class against Defendant NRS)

291. Plaintiff re-alleges and incorporates by reference paragraphs 1–240 above as if fully set forth herein, and bring this claim against Defendant NRS.

292. This Count is alleged in the alternative to Count II.

293. NRS entered into uniform written contracts with its clients, including Vitruvian Health, to provide third-party debt collection services.

294. Pursuant these contracts, NRS received from its clients and maintained Plaintiff's and Class Members' Private Information in the course of performing its contractual services, which it could not perform without receiving and maintaining such Private Information.

295. Pursuant to these contracts, NRS's clients, including Vitruvian Health, agreed to provide NRS with compensation and Plaintiff's and Class Members' Private Information.

296. In exchange, NRS agreed, in part, to implement adequate data security measures to safeguard Plaintiff's and Class Members' Private Information from unauthorized disclosure, and to timely notify Plaintiff and Class Members of the Data Breach.

297. NRS was required by statutes and regulations, including but not limited to the FTC Act, HIPAA, and state consumer privacy and protection laws, to have contracts with its clients that required NRS to implement and maintain reasonable security procedures and practices to protect its clients' customers'—Plaintiff and Class Members—Private Information from unauthorized access, use, or disclosure.

298. The relevant statutes and regulations obligating NRS to promise by contract to use reasonable data security for Plaintiff's and Class Members' Private Information create a class of intended beneficiaries whose members are implied into such agreements by operation of law. Plaintiff and Class Members are the intended beneficiaries of the contracts that NRS entered into.

299. Upon information and belief, NRS's contracts with its clients each contained a provision requiring NRS to implement and maintain reasonable security procedures and practices appropriate to the nature of Private Information NRS collected, to protect the Private Information from unauthorized access, use, or disclosure.

300. These contracts between NRS and its clients were made expressly for the benefit of Plaintiff and Class Members as the intended third-party beneficiaries of these contracts.

301. NRS knew Plaintiff and Class Members were involved and would benefit from the transactions that were subject to these contracts between NRS's clients and NRS.

302. NRS knew that if it breached its contractual obligation to adequately safeguard Plaintiff's and Class Members' Private Information, Plaintiff and Class Members would be harmed.

303. NRS breached these contracts with entities such as Vitruvian Health, by, among other acts and omissions: (a) failing to use reasonable data security measures, (b) failing to implement adequate protocols and employee training sufficient to protect Plaintiff's and Class

Members' Private Information from unauthorized disclosure, and (c) failing to promptly or adequately notify Plaintiff and Class Members of the Data Breach.

304. As a direct and proximate result of NRS's breaches of these contracts with its clients, Plaintiff and Class Members have suffered and will continue to suffer injuries as set forth herein and are entitled to damages sufficient to compensate for the losses they sustained.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class against all Defendants)

305. Plaintiff re-alleges and incorporates by reference paragraphs 1–240 above as if fully set forth herein, and bring this claim against all Defendants.

306. Plaintiff pleads this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein, to the extent Plaintiff and Class Members may not have an adequate remedy at law against Defendants.

307. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they provided their Private Information to Defendants. In exchange, Plaintiff and Class Members should have had their Private Information protected with adequate data security. Without the collection and receipt of Plaintiff's and the Class's Private Information, Defendants would not be able to provide services and would be unable to obtain revenue.

308. Defendants knew Plaintiff and Class Members conferred a benefit upon them and accepted and retained that benefit by accepting and retaining the Private Information entrusted to them, and indeed, generating revenue from doing so. Defendants profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

309. Defendants failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

310. Defendants acquired the Private Information through inequitable means as they failed to investigate and/or disclose the inadequate data security practices as alleged herein.

311. NRS enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information.

312. Vitruvian Health enriched itself by saving the costs it reasonably should have expended on a vendor and/or independent contractor with adequate data security measures to secure Plaintiff's and Class Members' Private Information

313. Instead of NRS providing a reasonable level of data security that would have prevented the Data Breach, and Vitruvian Health utilizing a vendor and/or independent contractor with a reasonable level of data security that would have prevented the Data Breach, Defendants calculated to increase their own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and vendors and/or independent contractors and diverting those funds to their own pockets. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decisions to prioritize their own profits over the requisite security of customers' Private Information.

314. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon them.

315. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injuries and damages as set forth herein.

316. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

COUNT V
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Nationwide Class against all Defendants)

317. Plaintiff re-alleges and incorporates by reference paragraphs 1–240 above as if fully set forth herein, and bring this claim against all Defendants.

318. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary supplemental relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

319. In the fallout of the Data Breach, a controversy has arisen about: (a) NRS's duties to use reasonable data security for the Private Information it collects and maintains; and (b) Vitruvian Health's duties to use vendors and/or independent contractors with reasonable data security for the Private Information it collects and maintains.

320. On information and belief, Defendants' actions were—and still are—inadequate and unreasonable. Plaintiff and Class Members continue to suffer injuries from the ongoing threat of fraud and identity theft due to NRS's inadequate data security measures and Vitruvian Health's failure to use vendors and/or independent contractors with adequate data security measures.

321. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring as follows:

a. NRS owed—and continues to owe—a legal duty to use reasonable data security to secure the Private Information entrusted to it;

b. Vitruvian Health owed—and continues to owe—a legal duty to ensure any vendors and/or contractors it hires use reasonable data security to secure the Private Information entrusted to it;

c. Defendants have a duty to notify impacted individuals of the Data Breach under common law, Section 5 of the FTC Act, and HIPAA;

d. NRS breached, and continues to breach, its duties by failing to use reasonable measures to protect the Private Information entrusted to it from unauthorized access, use, and disclosure

e. Vitruvian Health breached, and continues to breach, its duties by failing to ensure the vendors and/or contractors it utilizes deploy adequate data security and/or by willingly using vendors and/or contractors who fail to use reasonable measures to protect the Private Information; and

f. Defendants' breaches of their duties caused—and continue to cause—injuries to Plaintiff and Class Members.

322. The Court should also issue injunctive relief requiring NRS to use adequate data security consistent with industry standards and Vitruvian Health to use vendors and/or independent contractors with adequate security consistent with industry standards.

323. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injuries and lack an adequate legal remedy if a second data breach occurs. And if a second breach occurs, Plaintiff and Class Members will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full, and they will be forced to bring multiple lawsuits

to rectify the same conduct. Simply put, monetary damages, while warranted for out-of-pocket damages and other legally quantifiable and provable damages, cannot cover the full extent of Plaintiff's and Class Members' injuries.

324. If an injunction is not issued, the resulting hardship for Plaintiff and Class Members far exceeds the minimal hardship that Defendants could experience if an injunction is issued.

325. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class Members, and the public at large.

COUNT VI
NEGLIGENT SELECTION, HIRING, OR RETENTION
(On behalf of Plaintiff and the Nationwide Class against Vitruvian Health)

326. Plaintiff re-alleges and incorporates by reference paragraphs 1–240 above as if fully set forth herein, and bring this claim against Vitruvian Health.

327. At all relevant times, NRS was Defendants' independent contractor. Vitruvian Health allowed NRS access to the Private Information of Plaintiff and the Class without: (a) vetting NRS and inquiring about its data security qualifications; (b) inquiring about and/or investigating NRS's data security procedures, protocols, and infrastructure; (c) ensuring NRS had data security systems and procedures compliant with HIPAA, the FTC Act, and recognized industry standards; (d) ensuring NRS adequately secured and protected Private Information in its possession from data breaches; and/or (e) advising NRS of the confidential nature of Plaintiff's and the Class's Private Information and its duty to protect that information.

328. If Vitruvian Health would have inquired into the adequacy of NRS's data security prior to selecting, retaining, and hiring NRS, Vitruvian Health would have known NRS was incompetent and incapable of adequately protecting and securing Plaintiff's and the Class's Private Information. Reason being, Vitruvian Health would have discovered NRS *did not* have data

security measures in place that were compliant with HIPAA, the FTC Act, and recognized industry standards. Under these circumstances, Vitruvian Health knew or should have known that NRS was incompetent.

329. However, Vitruvian Health was negligent and failed to exercise the requisite standard of care in the hiring, selecting, and retaining NRS.

330. Vitruvian Health owed a duty to Plaintiff and the Class to ensure NRS had adequate data security, procedures, and protocols sufficient to protect Plaintiff's and the Class's Private Information from data breaches prior to hiring NRS.

331. Vitruvian Health also owed a continuing duty to Plaintiff and the Class to ensure NRS continued to employ adequate data security, procedures, and protocols sufficient to protect Plaintiff's and the Class's Private Information from data breaches after hiring NRS.

332. Vitruvian Health breached these duties by failing to ensure NRS possessed the requisite data security, procedures, practices, infrastructure, and protocols to protect Plaintiff's and the Class's Private Information from data breaches prior to hiring NRS and while NRS worked for Vitruvian Health.

333. Additionally, Vitruvian Health breached its duties and obligations by: (a) failing to ensure NRS designed, implemented, monitored, and maintained reasonable network safeguards against foreseeable threats; (b) failing to ensure NRS designed, implemented, and maintained reasonable data retention policies; (c) failing to ensure NRS adequately trained or oversaw its employees regarding data security; (d) failing to ensure NRS complied with industry standard data security practices; (e) failing to ensure NRS encrypted or adequately encrypted the Private Information that was stored on NRS's network; (f) failing to ensure NRS had systems or processes in place to recognize or detect that NRS's network had been compromised and accessed; (g) failing

to ensure NRS utilized widely available software able to detect and prevent data breaches; and (h) failing to ensure NRS otherwise adequately secured the Private Information of Plaintiff and the Class using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

334. Vitruvian Health was on notice of the importance of data security because of well-publicized data breaches occurring throughout the United States. Despite knowledge of prior data breaches, Vitruvian Health failed to ensure NRS possessed the requisite data security posture to protect Plaintiff's and the Class's Private Information from unauthorized disclosure.

335. Vitruvian Health knew or should have known that the failure to ensure NRS employed adequate data security, procedures, and protocols would create an unreasonable risk of danger to persons and property.

336. As a direct and proximate result of Vitruvian Health's breach of its duties, and its negligent hiring, retention, and selection of NRS, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, diminution in value of their Private Information, and actual misuse of their Private Information.

337. Vitruvian Health was advised of the Data Breach, but continued to employ NRS, putting Plaintiff and the Class at risk of more data breaches in the future.

338. The acts and omissions of Vitruvian Health in negligently hiring, retaining, and/or selecting NRS are such as to show gross negligence and reckless disregard for the safety of others and, therefore, punitive damages are appropriate.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and all others similarly situated, pray for judgment as follows:

A. An Order certifying this case as a class action on behalf of Plaintiff and the proposed Classes, appointing Plaintiff as class representatives, and appointing their counsel to represent the Classes;

B. Awarding Plaintiff and the Classes damages that include applicable compensatory, actual, statutory, nominal, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiff and the Classes in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Classes;

E. Awarding injunctive relief in the form of additional technical and administrative cybersecurity controls as is necessary to protect the interests of Plaintiff and the Classes;

F. Enjoining Defendants from further deceptive practices and making untrue statements about their data security, the Data Breach, and the transmitted Private Information;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law; and

I. Awarding such further relief to which Plaintiff and the Classes are entitled.

IX. DEMAND FOR JURY TRIAL

Plaintiff demand a trial by jury on all issues to triable.

Date: April 22, 2025

Respectfully submitted,

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV (BPR 23045)
Grayson Wells (BPR 039658)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Ave., Ste. 200
Nashville, TN 37203
Tel: (615) 254-8801
Fax: (615) 255-5419
gstranch@stranchlaw.com
gwells@stranchlaw.com

William B. Federman*
Kennedy M. Brian*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Ph: (405) 235-1560
F: (405) 239-2112
Email: wbf@federmanlaw.com

**Pro Hac Vice Application Forthcoming*

Attorneys for Plaintiff and Proposed Class