

Adam T. Savett  
Matthew Insley-Pruitt (*pro hac vice* forthcoming)  
Justyn J. Millamena (*pro hac vice* forthcoming)  
WOLF POPPER LLP  
570 Lexington Ave., 19th Floor  
New York, NY 10022  
Tel: (212) 759-4600  
ASavett@wolfpopper.com  
MInsley-Pruitt@wolfpopper.com  
JMillamena@wolfpopper.com

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW JERSEY**

FELICIA BILLINGSLEA, MICHAEL  
CONRAD, CHAREIN FARAJ,  
MICHELLE LEY, and STACEY  
MARCHAND, individually and on behalf  
of all others similarly situated,

Plaintiffs,

v.

COGNIZANT TECHNOLOGY  
SOLUTIONS CORPORATION,  
TRIZETTO PROVIDER SOLUTIONS,  
LLC,

Defendants.

Case No.: 2:26-cv-3394

JURY TRIAL DEMANDED

**CORRECTED CLASS ACTION COMPLAINT**

Plaintiffs Felicia Billingslea, Michael Conrad, Charein Faraj, Michelle Ley, and Stacey Marchand (“Plaintiffs”), individually and on behalf of all others similarly situated, bring this class action against Defendants Cognizant Technology Solutions Corporation (“Cognizant”), at 300 Frank W Burr Blvd, Suite 600,

Teaneck, NJ 07666, and TriZetto Provider Solutions, LLC (“TriZetto” or “TPS”), 3300 Rider Trail S., Earth City, Missouri 63045 (collectively, “Defendants”).

Plaintiffs bring this action by and through their attorneys, and allege, based upon personal knowledge as to their own actions, and based upon information and belief and reasonable investigation by their counsel as to all other matters, as follows.

### **INTRODUCTION**

1. Defendant Cognizant owns and operates several companies that provide software solutions to stakeholders in the health care industry, such as health care providers, health insurers, and others. Its wholly-owned subsidiary, Defendant TriZetto, provides revenue cycle management services to physician practices. This includes assisting with the claims management process, where providers submit claims to third-party payers such as insurance companies, and assisting with appeals if the insurance company denies a claim. TriZetto says that it is “fueled by Cognizant” and supports over 200 million lives.<sup>1</sup>

2. In order to perform this role, Cognizant and TriZetto handle vast amounts of confidential and sensitive information. This includes both “personally identifying information” (“PII”) such as name, birthday, and billing information, as well as “protected health information” (“PHI”, together with PII, “Private

---

<sup>1</sup> <https://www.trizettoprovider.com/who-we-are/our-story>;  
<https://www.trizettoprovider.com/who-we-serve/physician-practices>.

Information”) such as health histories, provider information, and health insurance information. Defendants are trusted by their provider clients and the patients to handle this information with due care and preserve its security.

3. Unfortunately, Defendants did not properly guard this Private Information. On October 2, 2025, TriZetto discovered suspicious activity in its system (the “Breach”). Specifically, an unauthorized actor began accessing patient Private Information as far back as November 2024. TriZetto determined that the intruders accessed patient records that included both PHI (including health information, provider information, and health insurance information) and PII (including name, birth date, and social security numbers). TriZetto disclosed that more than 3.4 million individuals were affected by the Breach.

4. The Breach occurred because Defendants did not take adequate measures to protect the Private Information they were trusted with and allowed the unauthorized access to continue undetected for roughly one year. Plaintiffs and the Class of other affected patients (as defined *infra*) have been harmed by this disclosure. First and foremost, few things are more sensitive and personal than information about one’s health, and courts recognize the special regard for personal health information under the law. Additionally, Plaintiffs and the Class have suffered injuries that include lost time and effort spent to investigate the potential disclosure of their Private Information, potential charges and fees

associated with the disclosure of the Private Information in the Breach, potential expenses related to dealing with mitigating the consequences of the Breach, and the continued heightened risk of fraud as a result of the Breach.

5. Plaintiffs bring this class action on behalf of themselves and all others similarly situated in the alleged Class to seek relief from the consequences of Defendants' failure to secure her Private Information.

### **PARTIES**

6. Plaintiff Felicia Billingslea is a resident and citizen of Massachusetts. Plaintiff Billingslea received notices from Defendant TriZetto informing her of the breach and that her minor sons' data were affected.

7. Plaintiff Michael Conrad is a resident and citizen of Massachusetts. Plaintiff Conrad received a notice from Defendant TriZetto informing him of the breach and that his data was affected.

8. Plaintiff Charein Faraj is a resident and citizen of Michigan. Plaintiff Faraj received a notice from Defendant TriZetto informing her of the breach and that her data was affected.

9. Plaintiff Michelle Ley is a resident and citizen of North Dakota. Plaintiff Ley received a notice from Defendant TriZetto informing him of the breach and that his data was affected.

10. Plaintiff Stacey Marchand is a resident and citizen of New Hampshire. Plaintiff Marchand received notices from Defendant TriZetto informing him of the breach and that his and his daughters' data were affected.

11. Defendant Cognizant is a Delaware corporation with its principal place of business located in Teaneck, NJ. Defendant Cognizant conducts business in New Jersey and throughout the United States.

12. Defendant TriZetto is a limited liability corporation with its principal place of business located in Earth City, Missouri. Defendant TriZetto conducts business in New Jersey and throughout the United States. TriZetto describes itself as a Cognizant company.

### **JURISDICTION AND VENUE**

13. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d), because this is a class action in which the matter in controversy exceeds the sum of \$5,000,000, the number of class members exceeds 100, and at least one Class member is a citizen of a state different from Defendants. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

14. This Court has personal jurisdiction over Defendants because Cognizant maintains its headquarters in the state of New Jersey, and because both Defendants regularly conduct business in this State.

15. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiffs' and Class members' claims occurred in this District.

### **FACTUAL ALLEGATIONS**

#### **Defendants' Business and Representations**

16. Cognizant is an information technology consulting and outsourcing company with more than \$20 billion in revenue each year. In 2014, Cognizant acquired TriZetto for \$2.4 billion.

17. TriZetto is a healthcare technology company that provides software solutions to healthcare providers, insurance companies, and other entities within the healthcare industry. TriZetto is a wholly owned subsidiary of Cognizant.

18. As part of the services that they provide to health care providers and others, Defendants collect, store, and process a huge amount of Private Information related to their customers' patients. In fact, TriZetto states that it supports more than 200 million lives.

19. Upon information and belief, Defendants failed to implement necessary data security safeguards at the time of the Breach. This failure resulted

in the exfiltration of Private Information of Defendants’ customers’ patients like Plaintiffs and other Class members.

20. Plaintiffs and Class members had the reasonable expectation that the Defendants would keep any Private Information that they received confidential and secure from illegal and unauthorized access. They also expected that entities like Defendants would provide them with prompt and accurate notice if the data were accessed by unauthorized parties.

21. This was a reasonable expectation. In fact, Defendant Cognizant advertises one of the services it provides as “Data Protection & Privacy Services,” and claims that “Cognizant offers comprehensive data protection and privacy services—safeguarding sensitive information, ensuring compliance and enhancing resilience through advanced data discovery, protection and monitoring solutions.”<sup>2</sup> Cognizant also admits that “Data breaches can cause severe financial and reputational damage.”

22. Similarly, in the “General Terms” of the agreements between TriZetto and its customers, TriZetto agrees to “use reasonable and appropriate safeguards” to protect PHI as contemplated by the HIPAA rules.<sup>3</sup> These specific safeguards are

---

<sup>2</sup> <https://www.cognizant.com/us/en/services/cybersecurity-services/data-protection-and-privacy-services>, archived at <https://perma.cc/5EUS-T98B>.

<sup>3</sup> General Terms, TriZetto, <https://www.trizettoprovider.com/wp-content/uploads/GeneralTerms05232017.pdf>, archived at <https://perma.cc/BKC4-UUEE>.

provided in the “business associate agreement” (“BAA”).<sup>4</sup> Among other representations, TriZetto states that it will “use reasonable and appropriate safeguards in compliance with Subpart C of 45 C.F.R. Part 164 with respect to PHI in electronic format designed to prevent use or disclosure of PHI”; it will not disclose PHI unless pursuant to law; and it will abide by HIPAA and other laws.

23. Furthermore, the “Privacy Policy” on the TriZetto website directs users to the “Privacy Notice” on the Cognizant website, which in turns claims to cover the TriZetto website.<sup>5</sup> The policy or notice claims that “Cognizant implements appropriate security measures designed to prevent unlawful or unauthorized processing of personal information and accidental loss of or damage to personal information.”

24. Defendants failed to protect Plaintiffs and the Class members’ Private Information and provide adequate data security. Defendants therefore failed to protect Plaintiffs and Class members from having their Private Information accessed and stolen during the Breach.

---

<sup>4</sup> Business Associate Agreement, TriZetto, <https://www.trizettoprovider.com/wp-content/uploads/BAA-05232017.pdf>, archived at <https://perma.cc/BV42-NBGY>.

<sup>5</sup> Cognizant Website Privacy Notice, Cognizant, <https://www.cognizant.com/us/en/privacy-notice>, archived at <https://perma.cc/7QQV-CJVU>.

## **The Breach**

25. TriZetto first identified suspicious activity in its web portal on October 2, 2025. Its subsequent investigation determined that the threat actors had been active in the web portal since at least November 2024, almost one year earlier. The breach affected the revenue cycle management records that were relevant to insurance eligibility verification.

26. TriZetto learned on November 28, 2025 that Private Information had been obtained, including name, address, date of birth, Social Security number, health insurance member number, provider name, health insurance name, primary insured information, and other demographic, health, and health insurance information.

27. TriZetto began informing its health care provider clients of the breach on December 9, 2025.

28. TriZetto informed state regulators, including the Office of the Attorney General of Maine, that it did not begin informing affected patients until February 6, 2025.<sup>6</sup>

---

<sup>6</sup> See <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/e2c4cc45-dc81-498d-89f0-28c887808b41.html>, archived at <https://perma.cc/36BV-86HB>.

29. As of the report to the Attorney General of Maine, TriZetto believed that more than 3.4 million people were affected. TriZetto has not indicated whether its review is complete.

30. While there have been thousands of data breaches each year for the last several years, and hundreds of data breaches involving healthcare data each year, the HIPAA Journal reported that the Breach was one of the largest data breaches to be confirmed this year, and the 37<sup>th</sup> largest healthcare data breach since 2009.<sup>7</sup>

31. The Breach was a direct, proximate, and foreseeable result of multiple failures by Defendants.

32. For example, Defendants failed to properly implement reasonable security protections for the Private Information. As a result, they failed to detect or stop the Breach in a timely manner, and allowed the unauthorized access for almost a full year. While Defendants claim that they prevented further unauthorized access once they became aware of the Breach, had they become aware of the Breach earlier it would have lessened or prevented the damage. The Defendants also did not inform the Plaintiffs and the Class that, despite their reassurances, their data security practices actually were insufficient.

---

<sup>7</sup> <https://www.hipaajournal.com/trizetto-provider-solutions-data-breach/> (last accessed March 13, 2026); <https://www.hipaajournal.com/healthcare-data-breach-statistics/> (last accessed March 13, 2026)

33. When notifying Plaintiffs and other members of the Class, Defendants offered to provide credit monitoring services for a limited period. However, credit monitoring will have less benefit to individuals whose PHI—including vague “health information”—have been compromised. Furthermore, medical records and other health information is reportedly worth multiple times the value of just financial information to criminal actors given its usefulness in medical identity theft and related harms.

34. The compounding impact of multiple data breaches like this Breach can damage Plaintiffs and Class members as more and more pieces of information become available to unsavory characters. For example, cybercriminals could use the Private Information to access, inter alia, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class members, even when that specific category of information is not compromised in a given breach.

### **Defendants Have Multiple Obligations To Protect the Private Information**

35. Defendants have a duty to protect the confidentiality of the Private Information that they hold.

36. As Defendants recognize, they have an obligation to have policies, procedures, and safeguards to protect PHI and PII pursuant to the requirements of HIPAA, 45 CFR § 164.302, *et seq.* The HIPAA regulations also require parties to

notify victims of a breach within 60 days of discovery of the breach, which Defendants did not do here.

37. Defendants failed to implement and/or maintain procedures, systems, and safeguards to protect the Private Information belonging to Plaintiffs and Class members from unauthorized access and disclosure.

38. Defendants also failed to store the information they collected in a manner that rendered it, “unusable, unreadable, or indecipherable to unauthorized persons,” in violation of 45 CFR § 164.402.

39. The Federal Trade Commission (“FTC”) has also issued similar guidelines and requirements for the preservation of confidential information in a secure manner. The Breach shows that Defendants failed to protect the Private Information in accordance with these guidelines or to institute appropriate data security measures.

40. Best practices and customs that are standard within the industry also require companies like Defendants to institute appropriate and effective controls and policies to protect PHI and PII like the Private Information. Defendants failed to follow these standards thereby allowed the Breach to occur.

### **Plaintiffs’ Experiences**

41. In or around February 2026, Plaintiff Billingslea received a notification letter (the “Letter”) in the mail from TriZetto for each of her minor

sons informing her of the Breach and that her sons' Private Information was included in the data accessed by unauthorized agents. An example of the Letter that was materially similar for all Plaintiffs is attached as Exhibit A.<sup>8</sup> The Letters did not provide reasonable specificity for a consumer whose Private Information—including “health” information—was disclosed. For example, the Letters did not even indicate which medical provider was a client of TriZetto and what nature of information was accessed. Plaintiff Billingslea uses several medical providers for her sons, but does not know what medical information is at stake. The Letters provided a link and password for Plaintiff Billingslea to obtain limited credit monitoring services for her sons.

42. In or around January 2026, Plaintiff Conrad received an overdue credit card notice from Capital One indicating that a card opened in his name had incurred a balance of \$3,000. Plaintiff Conrad had not opened the account. Thereafter, he contacted Capital One and credit agencies to close the account and report the fraud. In or around February 2026, Plaintiff Conrad received a Letter in

---

<sup>8</sup> In a letter provided to the Office of the Attorney General of California that was an exemplar of the letters sent to affected business partners in December 2025, TriZetto stated that it would notify “customers that were affected” directly, and that notification letters would be sent “to affected individuals.”

<https://oag.ca.gov/system/files/TPS%20Letter%20to%20Affected%20Business%20Partners.pdf>, archived at <https://perma.cc/VY7F-5KJR>. While the Letter that Plaintiffs received says that their data “may have involved some of [her] protected health information” and does not provide specific detail of which categories of Private Information were obtained (Ex. A), it is reasonable to assume that their data was accessed without authorization because TriZetto made the considered decision to send them the Letter.

the mail from TriZetto informing him of the Breach and that his Private Information was included in the data accessed by unauthorized agents. Aside from the TriZetto Letter, Plaintiff Conrad has not received any other notice that his Private Information was compromised. The Letter did not provide reasonable specificity for a consumer whose Private Information—including “health” information—was disclosed. For example, the Letter did not even indicate which medical provider was a client of TriZetto and what nature of information was accessed. Plaintiff Conrad has several medical providers, but does not know what medical information is at stake. The Letter provided a link and password for Plaintiff Conrad to obtain limited credit monitoring services.

43. In or around February 2026, Plaintiff Faraj received a Letter in the mail from TriZetto informing her of the Breach and that her Private Information was included in the data accessed by unauthorized agents. The Letter did not provide reasonable specificity for a consumer whose Private Information—including “health” information—was disclosed. For example, the Letter did not even indicate which medical provider was a client of TriZetto and what nature of information was accessed. Plaintiff Faraj has several medical providers, but does not know what medical information is at stake. The Letter provided a link and password for Plaintiff Faraj to obtain limited credit monitoring services.

44. In or around February 2026, Plaintiff Ley received a Letter in the mail from TriZetto informing him of the Breach and that his Private Information was included in the data accessed by unauthorized agents. The Letter did not provide reasonable specificity for a consumer whose Private Information—including “health” information—was disclosed. For example, the Letter did not even indicate which medical provider was a client of TriZetto and what nature of information was accessed. Plaintiff Ley has several medical providers, but does not know what medical information is at stake. The Letter provided a link and password for Plaintiff Ley to obtain limited credit monitoring services.

45. In or around February 2026, Plaintiff Marchand received Letters in the mail from TriZetto informing him of the Breach and that his and his daughter’s Private Information was included in the data accessed by unauthorized agents. The Letters did not provide reasonable specificity for a consumer whose Private Information—including “health” information—was disclosed. For example, the Letters did not even indicate which medical provider was a client of TriZetto and what nature of information was accessed. Plaintiff Marchand and his daughter have several medical providers, but do not know what medical information is at stake. The Letters provided a link and password for Plaintiff Ley to obtain limited credit monitoring services.

46. Plaintiffs suffered actual injury from their Private Information compromised as a result of the Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendants obtained from them; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

### **CLASS ALLEGATIONS**

47. Plaintiffs bring this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Nationwide Class of:

All persons in the United States whose Private Information was accessed in the Breach.

48. Plaintiffs Billingslea and Conrad also bring this action on behalf of a subclass of:

All persons in Massachusetts whose Private Information was accessed in the Breach (the “Massachusetts Subclass”).

49. Plaintiff Faraj also brings this action on behalf of a subclass of:

All persons in Michigan whose Private Information was accessed in the Breach (the “Michigan Subclass”).

50. Plaintiff Ley also brings this action on behalf of a subclass of:

All persons in North Dakota whose Private Information was accessed in the Breach (the “North Dakota Subclass”).

51. Plaintiff Marchand also brings this action on behalf of a subclass of:

All persons in New Hampshire whose Private Information was accessed in the Breach (the “New Hampshire Subclass”).

52. Unless specifically indicated otherwise, all allegations below concerning the Nationwide Class include and equally apply to all the Subclasses, individually and collectively. The Nationwide Class and the Subclasses are collectively referred to as the “Class.”

53. Excluded from the Class are Defendants, their executives and officers, and the Judge(s) assigned to this case. Plaintiffs reserve the right to modify, change or expand the Class definition after conducting discovery.

54. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendants and obtainable by Plaintiffs only through the discovery process. However, notice of the breach provided by TriZetto to the Maine Attorney General’s Office indicated that there were more than 3.4 million persons affected.<sup>9</sup>

55. Common Questions of Law and Fact: Common questions of law and fact exist as to all members of the Class. These questions predominate over the

---

<sup>9</sup> <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/e2c4cc45-dc81-498d-89f0-28c887808b41.html>, archived at <https://perma.cc/36BV-86HB>.

questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

- a. When Defendants learned of the Breach;
- b. Whether Defendants adequately responded to the Breach;
- c. What Private Information was obtained in the Breach;
- d. Whether reasonable security procedures were implemented prior to the Breach;
- e. Whether Defendants owed a duty to the Class members to safeguard their Private Information;
- f. Whether Defendants breached this duty to safeguard the Private Information;
- g. Whether Defendants had a duty to disclose the Breach to Class members in a timely manner;
- h. Whether Defendants breached this duty to disclose the Breach in a timely manner;
- i. Whether Defendants knew or should have known that the safety procedures with respect to the Private Information were inadequate;
- j. Whether Defendants' conduct violated the FTCA and/or HIPAA;
- k. Whether Defendants' conduct was negligent;
- l. Whether Defendants were unjustly enriched;
- m. What damage Plaintiffs and Class members suffered as a result of Defendants' misconduct; and
- n. Whether Plaintiffs and Class members are entitled to actual and/or statutory damages.

56. Typicality: Plaintiffs' claims are typical of the claims of the Class as

Plaintiffs and all members of the Class had their Private Information compromised in the Breach. Plaintiffs' claims and damages are also typical of the Class because they resulted from Defendants' uniform wrongful conduct. Likewise, the relief to

which Plaintiffs are entitled to is typical of the Class because Defendants have acted, and refused to act, on grounds generally applicable to the Class.

57. Adequacy: Plaintiffs are adequate class representatives because their interests do not materially or irreconcilably conflict with the interests of the Class they seek to represent, they have retained counsel competent and highly experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Neither Plaintiffs nor their counsel have any interests that are antagonistic to the interests of other members of the Class.

58. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class, a class action is superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendants' conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far

fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, inter alia, Defendants' records and databases.

**APPLICABILITY OF MASSACHUSETTS  
GENERAL LAW CHAPTER 93A**

59. The Massachusetts Regulation of Business Practice and Consumer Protection Act prohibits unfair and deceptive acts or practices in the conduct of trade or commerce. Mass. Gen. L. ch. 93A, § 2(a).

60. Plaintiffs Billingslea and Conrad and Massachusetts Class members are "persons" within the meaning of ch. 93A, § 1(b).

61. Defendants engaged in "trade" or "commerce" within the meaning of ch. 93A, § 1(b).

62. Plaintiffs Billingslea and Conrad and other Class members are consumers whose Private Information was processed by Defendants and accessed in the Breach.

63. Defendants' conduct, as described above, constitutes an unfair and deceptive practice and was likely to mislead a reasonable consumer.

64. Defendants' conduct, as alleged herein, is in violation of the regulations promulgated by the Massachusetts Attorney General under ch. 93A, including but not limited to: 940 C.M.R. § 3.05(1) (prohibiting claims or

representations “made by any means concerning a product which, directly, or by implication, or by failure to adequately disclose additional relevant information, has the capacity or tendency or effect of deceiving buyers or prospective buyers in any material respect”); 940 C.M.R. § 3.08(2) (providing that it “shall be an unfair and deceptive act or practice to fail to perform or fulfill any promises or obligation arising under a warranty”); and 940 C.M.R. § 3.16(2) (providing that it is a violation of ch. 93A, § 2 to “fail to disclose to a buyer or prospective buyer any fact, the disclosure of which may have influenced the buyer or prospective buyer to enter into the transaction”).

65. Defendants’ deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs Billingslea and Conrad’s and the Massachusetts Subclass’s Private Information, which was a direct and proximate cause of the Breach.
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Billingslea and Conrad’s and Massachusetts Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs Billingslea and Conrad’s and Massachusetts Subclass members’ Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs

Billingslea and Conrad's and Massachusetts Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

- f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs Billingslea and Conrad's and Massachusetts Subclass members' Private Information; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Billingslea and Conrad's and Massachusetts Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

66. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs Billingslea and Conrad and Massachusetts Subclass members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

67. Defendants (1) represented in their policies that they were implementing reasonable security measures to protect Plaintiffs Billingslea and Conrad's and Massachusetts Subclass members' sensitive personal information and (2) failed to implement reasonable data security measures.

68. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiffs Billingslea and Conrad and Massachusetts Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid for goods and services or would have paid less for such goods and services but for Defendants'

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

69. Plaintiffs Billingslea and Conrad will provide notice to Defendants pursuant to Massachusetts General Law Chapter 93A that they intend to seek appropriate monetary and non-monetary relief as allowed by law, including injunctive relief, actual damages, restitution, attorneys' fees, and any other appropriate relief.

## **CLAIMS FOR RELIEF**

### **Count I**

#### Negligence / Negligence Per Se

(On Behalf of Plaintiffs and the Nationwide Class and the Subclasses)

70. Plaintiffs restate and reallege all the factual allegations in paragraphs 1 through 69, as if fully set forth herein.

71. Defendants knowingly collected, possessed, and maintained Plaintiffs' and Class Members' Private Information, and therefore had a duty to exercise reasonable care in safeguarding, securing, and protecting such Private Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

72. Defendants' duty also included a responsibility to implement processes by which they could detect and analyze a breach of their security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

73. Defendants knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Defendants were on notice because they knew or should have known that they would be an attractive target for cyberattacks.

74. Defendants owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to them. Defendants' duties included, but were not limited to, the following:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in their possession;
- b. To protect the Private Information in their possession by using reasonable and adequate security procedures and systems compliant with industry standards;
- c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in their possession;
- d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to HIPAA and the FTCA;
- e. To adequately and properly oversee third party vendors in which sensitive Private Information is entrusted;
- f. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

- g. To promptly notify Plaintiffs and Class Members of the Breach, and to precisely disclose the type(s) of information compromised.

75. Defendants' duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission 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.

76. Pursuant to Section 5 of the FTCA, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

77. Defendants' duty to implement reasonable safeguards also arose, in part, under HIPAA, 42 U.S.C. § 1302(d), *et seq.*, pursuant to which, Defendants had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

78. Defendants' duty also arose because Defendants were bound by industry standards to protect the confidential Private Information entrusted to them.

79. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendants, and Defendants owed them a duty of care to not subject them to an unreasonable risk of harm.

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

81. Defendants, by their actions and/or omissions, breached their duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

82. Defendants, by their actions and/or omissions, breached their duty of care by failing to promptly identify the Breach and then failing to provide prompt notice of the Breach to the persons whose Private Information was compromised.

83. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

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

- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to periodically ensure that their email system maintained reasonable data security safeguards;
- d. Allowing unauthorized access to Plaintiffs' and Class Members' Private Information;
- e. Failing to comply with the FTCA and HIPAA;
- f. Failing to detect in a timely manner that Plaintiffs' and Class Members' Private Information had been compromised; and
- g. Failing to timely notify Plaintiffs' and Class Members about the Breach so they could take appropriate steps to mitigate the potential for identity theft and other damages.

84. Defendants breached their duties to Plaintiffs and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

85. Specifically, Defendants breached their duties by failing to employ industry-standard cybersecurity measures to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

86. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Breach). The FTC rulings and publications

described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Defendant's duty in this regard.

87. Defendants also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiffs and Class Members and by not complying with applicable industry standards, as described herein.

88. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendants' networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

89. Defendants acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Breach such that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Breach.

90. Defendants had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Defendants with their Private Information was predicated on the understanding that Defendants

would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems (and the Private Information that they stored on them) from attack.

91. Defendants' breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated, as alleged herein.

92. Defendants' breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and loss of time and money to monitor their accounts for fraud.

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

94. Defendants also had independent duties under state laws that required them to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Breach.

95. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

96. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

97. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

98. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, inter alia, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

## **Count II**

### Breach of Contract

(On Behalf of Plaintiffs and the Nationwide Class and the Subclasses)

99. Plaintiffs restate and reallege all the factual allegations in paragraphs 1 through 69, as if fully set forth herein.

100. Defendants and Defendants' clients contracted for revenue cycle management services, among other things. Defendants' clients include healthcare providers and health insurers.

101. As a condition of using Defendants' services, Defendants and Defendants' clients required Plaintiffs and Class Members to provide their Private Information.

102. When Plaintiffs and Class Members provided their Private Information to Defendants and Defendants' clients, they became third-party beneficiaries to these contracts, pursuant to which Defendants agreed to safeguard and protect such Private Information and to timely and accurately notify Plaintiffs and Class Members if and when their Private Information was breached and compromised.

103. Specifically, Plaintiffs and Class Members were the intended or foreseeable third-party beneficiaries of these contracts between Defendants and Defendants' clients when Plaintiffs and Class Members agreed to provide their Private Information and/or payment to their medical providers.

104. Defendants represented in their privacy policies and notices, as well as agreements with providers, that they would take appropriate measures to ensure the security of the Private Information.

105. Further, Defendants promised and warranted to Plaintiffs and Class Members, including through their public-facing privacy documents, to maintain the privacy and confidentiality of the Private Information it collected from Plaintiffs and Class Members and to keep such information safeguarded against unauthorized access and disclosure.

106. Defendants' adequate protection of Plaintiffs' and Class Members' Private Information was a material aspect of these contracts, to which Plaintiffs and Class Members were the intended or foreseeable third-party beneficiaries.

107. In providing their Private Information to Defendants and Defendants' clients, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with industry standards and relevant laws and regulations, including the FTC Act, HIPAA, and with industry standards.

108. Plaintiffs and Class Members would not have provided their Private Information to Defendants and Defendants' clients had they known that Defendants would not safeguard their Private Information.

109. Defendants breached the contracts they entered by failing to safeguard and protect Plaintiffs' and Class Members' Private Information, failing to delete the information of Plaintiffs and Class Members once the relationship ended, and failing to provide timely and accurate notice to them that their Private Information was compromised as a result of the Breach.

110. The Breach was a reasonably foreseeable consequence of Defendants' conduct, by acts of omission or commission, in breach of these contracts, to which Plaintiffs and Class Members were the intended or foreseeable third-party beneficiaries.

111. As a result of Defendants' failures to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive the full benefit of their bargains with Defendants and Defendants' clients and instead received services of a diminished value compared to that described in the contracts. Plaintiffs 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 paid for and that which they received.

112. As a direct and proximate result of Defendants' breach of their contracts with Defendants' clients, to which Plaintiffs and Class Members were the intended or foreseeable third-party beneficiaries, and the attendant Breach, Plaintiffs and Class Members have suffered injuries and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they struck with Defendants and Defendants' clients. Plaintiffs and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports;

expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

113. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or restitution, in an amount to be proven at trial.

### **Count III**

#### **Unjust Enrichment**

(On Behalf of Plaintiffs and the Nationwide Class and the Subclasses)

114. Plaintiffs restate and reallege all the factual allegations in paragraphs 1 through 69, as if fully set forth herein.

115. Plaintiffs and Class Members conferred a benefit on Defendants by permitting TriZetto and Cognizant's Clients to turn over their Private Information to Defendants. Moreover, upon information and belief, Plaintiffs and Class Members allege that payments made by their medical providers to TriZetto and/or Cognizant included payment for cybersecurity protection to protect Plaintiffs' and Class Members' Private Information, and that those cybersecurity costs were passed on to Plaintiffs and Class Members in the form of elevated prices charged by the Clients for their services. But Plaintiffs and Class Members did not receive such protection.

116. Upon information and belief, Defendants fund their data security measures entirely from its general revenue, including, in the case of TriZetto and

Cognizant, from payments made to it by their Clients on behalf of Plaintiffs and Class Members.

117. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

118. Defendants have retained the benefits of their unlawful conduct, including the amounts of payment received indirectly from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

119. Defendants knew that Plaintiffs and Class Members conferred a benefit upon them, which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments they received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Breach.

120. If Plaintiffs and Class Members had known that Defendants had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendants.

121. Due to Defendants' conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendants to be permitted to retain the benefit of their wrongful conduct.

122. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private

Information compromised as a result of the Breach for the remainder of the lives of Plaintiffs and Class Members.

123. Plaintiffs 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 Plaintiffs and Class Members may seek restitution or compensation.

124. Plaintiffs and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

**Count IV**

Violations of Massachusetts Right to Privacy Law

Mass. Gen. Laws, ch. 214 § 1B

(On Behalf of Plaintiffs Billingslea and Conrad and the Massachusetts Subclass)

125. Plaintiffs Billingslea and Conrad restate and reallege all the factual allegations in paragraphs 1 through 69, as if fully set forth herein.

126. Mass. Gen. Laws, ch. 214, § 1B provides in relevant part that “[a] person shall have a right against unreasonable, substantial or serious interference with his privacy.”

127. Pursuant to ch. 214, § 1B, Defendants owed a legal duty of care to Plaintiffs Billingslea and Conrad and Class Members whose Private Information

was entrusted to them. Defendants' duties included, but were not limited to safeguarding, securing, and protecting the Private Information in their possession and keeping such Private Information confidential.

128. Plaintiffs Billingslea and Conrad and Class Members provided and entrusted Defendants and Defendants' clients with Private Information with the understanding that Defendants would safeguard, secure, and protect such Private Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

129. Plaintiffs Billingslea and Conrad and Class Members did not authorize Defendants to disclose their Private Information to the unauthorized parties who accessed such Private Information in the Breach.

130. Defendants failed to protect Plaintiffs Billingslea and Conrad and Class Members' highly sensitive Private Information, allowing unauthorized parties to access it, which constitutes an unreasonable and substantial invasion of privacy that is highly offensive to any reasonable person.

131. As a direct and proximate result of Defendants' breaches of duty, Plaintiffs Billingslea and Conrad and Class Members suffered damages as alleged herein and are at imminent risk of further harm.

132. Accordingly, Plaintiffs Billingslea and Conrad and Class Members seek compensatory damages plus costs and attorneys' fees. *See* ch. 214, § 1B.

**Count V**

Violation of the Michigan Consumer Protection Act,  
Mich. Comp. Laws Ann. § 445.091, *et seq.*  
(On Behalf of Plaintiff Faraj and the Michigan Subclass)

133. Plaintiff Faraj restates and realleges all the factual allegations in paragraphs 1 through 69, as if fully set forth herein.

134. The Michigan Consumer Protection Act (“Michigan CPA”) provides that “[u]nfair, unconscionable, or deceptive methods, acts or practices in the conduct of trade or commerce are unlawful . . .” Mich. Comp. Laws Serv. § 445.903(1).

135. Plaintiff and Defendants are each a “person” as defined in the Michigan CPA, Mich. Comp. Laws Serv. § 445.902(1)(d).

136. Defendants’ conduct constitutes “trade” or “commerce” as defined in the Michigan CPA, Mich. Comp. Laws Serv. § 445.902(1)(g).

137. As described above, while engaging in trade or commerce within the State of Michigan during the time period relevant hereto, Defendants engaged in the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff Faraj’s and the Michigan Subclass’s Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to periodically ensure that their email system maintained reasonable data security safeguards;

- d. Allowing unauthorized access to Plaintiff Faraj's and the Michigan Subclass's Private Information;
- e. Failing to comply with the FTCA and HIPAA;
- f. Failing to detect in a timely manner that Plaintiff Faraj's and the Michigan Subclass's Private Information had been compromised; and
- g. Failing to timely notify Plaintiff Faraj's and the Michigan Subclass's about the Breach so they could take appropriate steps to mitigate the potential for identity theft and other damages.

138. The aforesaid methods, acts, and practices constitute unfair,

unconscionable, or deceptive acts or practices in the conduct of any trade or

commerce in violation of the Michigan CPA, including, but not limited to, the

following:

- a. "Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has sponsorship, approval, status, affiliation, or connection that he or she does not have." (Mich. Comp. Laws Serv. § 445.903(1)(c));
- b. "Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another." (Mich. Comp. Laws Serv. § 445.903(1)(e));
- c. "Making a representation of fact or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is." (Mich. Comp. Laws Serv. § 445.903(1)(bb)); and
- d. "Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner." (Mich. Comp. Laws Serv. § 445.903(1)(cc)).

139. Defendants' conduct further violates the Michigan CPA by failing to comply with Michigan's Identity Theft Protection Act ("MITPA"), which required

Defendants to notify Plaintiff Faraj and the Michigan Subclass of the Breach “without reasonable delay.” Mich. Comp. Laws Ann. § 445.72(1), (4).

140. Plaintiff Faraj’s and the Michigan Subclass’s Private Information compromised in the Breach includes “personal information” as covered the MITPA, Mich. Comp. Laws Ann. § 445.72(1)(a).

141. Defendants are each a “person or agency that owns or licenses data” as defined by the MITPA, Mich. Comp. Laws Ann. § 445.72(1)(a).

142. As stated above, Defendants identified suspicious activity in its web portal on October 2, 2025, and subsequently learned that Private Information was obtained on November 28, 2025. Although Defendants had an obligation to disclose such in a timely fashion, Defendants did not notify the Plaintiffs and the Class until approximately February 6, 2026, approximately four months after it discovered the Data Breach and three months after it confirmed that Private Information had been compromised. This delay prevented Plaintiff Faraj from taking reasonable steps to safeguard her Private Information from identity theft, fraud, and future harm.

143. Plaintiff Faraj and the other members of the Michigan Subclass have been and continue to be injured as a direct and proximate result of Defendants’ violations of the Michigan CPA.

144. Defendants' conduct constitutes fraud and is gross, oppressive, aggravated, and involves breach of trust or confidence.

145. Plaintiff Faraj on behalf of herself and the Michigan Subclass, seeks actual damages, injunctive relief, other equitable relief, costs, and attorneys' fees as permitted by Mich. Comp. Laws Serv. § 445.911.

**Count VI**

Violation of the North Dakota Consumer Fraud Act,  
N.D. Cent. Code § 51-15-01, *et seq.*  
(On Behalf of Plaintiff Ley and the North Dakota Subclass)

146. Plaintiff Ley restates and realleges all the factual allegations in paragraphs 1 through 69, as if fully set forth herein

147. The North Dakota Consumer Fraud Act ("North Dakota CFA") makes unlawful "[t]he act, use, or employment by any person of any deceptive act or practice, fraud, false pretense, false promise, or misrepresentation, with the intent that others rely thereon in connection with the sale or advertisement of any merchandise." N.D. Cent. Code § 51-15-02.

148. Plaintiff Ley and Defendants are "persons" as defined in the North Dakota CFA, § 51-15-02(4).

149. Defendants engaged in the "sale" of "merchandise," including services, within the meaning of North Dakota CFA, § 51-15-01(3), (5).

150. As described above, while engaging in trade or commerce within the State of North Dakota during the time period relevant hereto, Defendants engaged in the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff Ley's and the North Dakota Subclass's Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to periodically ensure that their email system maintained reasonable data security safeguards;
- d. Allowing unauthorized access to Plaintiff Ley's and the North Dakota Subclass's Private Information;
- e. Failing to comply with the FTCA and HIPAA;
- f. Failing to detect in a timely manner that Plaintiff Ley's and the North Dakota Subclass's Private Information had been compromised; and
- g. Failing to timely notify Plaintiff Ley and the North Dakota Subclass about the Breach so they could take appropriate steps to mitigate the potential for identity theft and other damages.

151. The aforesaid methods, acts, and practices constitute unfair, unconscionable, or deceptive acts or practices in the conduct of any trade or commerce in violation of the North Dakota CFA.

152. Defendants' conduct further violates the North Dakota CFA by failing to comply with the North Dakota Notice of Security Breach for Personal Information Statute ("North Dakota NSB"), which required Defendants to notify Plaintiff Ley and the North Dakota Subclass of the Breach "in the most expedient time possible and without unreasonable delay." N.D. Cent. Code § 51-30-02.

153. Plaintiff Ley's and the North Dakota Subclass's Private Information compromised in the Breach includes "health insurance information," "medical information," and "personal information" as defined in the North Dakota NSB, N.D. Cent. Code § 51-30-01.

154. Defendants are each a "person that owns or licenses computerized data that includes personal information" as defined in the North Dakota NSB, N.D. Cent. Code § 51-30-02.

155. As stated above, Defendants identified suspicious activity in its web portal on October 2, 2025, and subsequently learned that Private Information was obtained on November 28, 2025. Although Defendants had an obligation to disclose such in a timely fashion, Defendants did not notify the Plaintiff and the Class until approximately February 6, 2026, approximately four months after it discovered the Data Breach and three months after it confirmed that Private Information had been compromised. This delay prevented Plaintiff from taking reasonable steps to safeguard his Private Information from identity theft, fraud, and future harm.

156. Plaintiff Ley and the other members of the North Dakota Subclass have been and continue to be injured as a direct and proximate result of Defendants' violations of the North Dakota CFA.

157. Defendants’ conduct constitutes fraud and is gross, oppressive, aggravated, and involves breach of trust or confidence.

158. Plaintiff Ley on behalf of himself and the North Dakota Subclass, seeks actual damages, injunctive relief, other equitable relief, costs, and attorneys’ fees.

**Count VII**

Violation of the New Hampshire Consumer Protection Act,  
N.H. Rev. Stat. Ann. § 358-A:1, *et seq.*

(On Behalf of Plaintiff Marchand and the New Hampshire Subclass)

159. Plaintiff Marchand restates and realleges all the factual allegations in paragraphs 1 through 69, as if fully set forth herein.

160. The New Hampshire Consumer Protection Act (“New Hampshire CPA”) provides that “[i]t shall be unlawful for any person to use any unfair method of competition or any unfair or deceptive act or practice in the conduct of any trade or commerce within this state.” N.H. Rev. Stat. Ann. § 358-A:2.

161. Defendants are “persons” as defined in the New Hampshire CPA, N.H. Rev. Stat. Ann. § 358-A:1.

162. Defendants’ conduct constitutes “trade” or “commerce” as defined in the New Hampshire CPA, N.H. Rev. Stat. Ann. § 358-A:1.

163. As described above, while engaging in trade or commerce within the State of New Hampshire during the time period relevant hereto, Defendants engaged in the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff Marchand's and the New Hampshire Subclass's Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to periodically ensure that their email system maintained reasonable data security safeguards;
- d. Allowing unauthorized access to Plaintiff Marchand's and the New Hampshire Subclass's Private Information;
- e. Failing to comply with the FTCA and HIPAA;
- f. Failing to detect in a timely manner that Plaintiff Marchand's and the New Hampshire Subclass's Private Information had been compromised; and
- g. Failing to timely notify Plaintiff Marchand's and the New Hampshire Subclass's about the Breach so they could take appropriate steps to mitigate the potential for identity theft and other damages.

164. The aforesaid methods, acts, and practices constitute unfair, unconscionable, or deceptive acts or practices in the conduct of any trade or commerce in violation of the New Hampshire CPA, including, but not limited to, the following:

- a. "Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that such person does not have" (N.H. Rev. Stat. Ann. § 358-A:2.V);
- b. "Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another" (N.H. Rev. Stat. Ann. § 358-A:2.VII); and
- c. "Advertising goods or services with intent not to sell them as advertised" (N.H. Rev. Stat. Ann. § 358-A:2.VII);

165. Defendants' conduct further violates the New Hampshire CPA by failing to comply with New Hampshire Notice of Security Breach Statute ("New Hampshire NSB"), which required Defendants to notify Plaintiff Marchand and the New Hampshire Subclass of the Breach "as soon as possible." N.H. Rev. Stat. § 359-C:20(I)(a).

166. Plaintiff Marchand and the other members of the New Hampshire Subclass have been and continue to be injured as a direct and proximate result of Defendants' violations of the New Hampshire CPA.

167. Defendants' conduct constitutes fraud and is gross, oppressive, aggravated, and involves breach of trust or confidence.

168. Plaintiff Marchand on behalf of himself and the New Hampshire Subclass, seeks actual damages, injunctive relief, other equitable relief, costs, and attorneys' fees.

### **Count VIII**

Violation of the New Hampshire Notice of Security Breach Statute,  
N.H. Rev. Stat. § 359-C:20, *et seq.*

(On Behalf of Plaintiff Marchand and the New Hampshire Subclass)

169. Plaintiff Marchand restates and realleges all the factual allegations in paragraphs 1 through 69, as if fully set forth herein.

170. The New Hampshire NSB provides that

Any person doing business in this state who owns or licenses computerized data that includes personal information, shall, when it becomes aware of a security breach, promptly determine the likelihood

that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible.

N.H. Rev. Stat. § 359-C:20(I)(a).

171. Plaintiff Marchand's and the New Hampshire Subclass's Private Information compromised in the Breach includes "personal information" as defined by the New Hampshire NSB, N.H. Rev. Stat. § 359-C:19(IV)(a).

172. Defendants are each a "person doing business in this state who owns or licenses computerized data" as defined by the New Hampshire NSB, N.H. Rev. Stat. § 359-C:20(I)(a).

173. As stated above, Defendants identified suspicious activity in its web portal on October 2, 2025, and subsequently learned that Private Information was obtained on November 28, 2025. Although Defendants had an obligation to disclose such in a timely fashion, Defendants did not notify the Plaintiffs and the Class until approximately February 6, 2026, approximately four months after it discovered the Data Breach and three months after it confirmed that Private Information had been compromised. This delay prevented Plaintiffs from taking reasonable steps to safeguard their Private Information from identity theft, fraud, and future harm.

174. Plaintiff Marchand and the other members of the New Hampshire Subclass have been and continue to be injured as a direct and proximate result of Defendants' violations of the New Hampshire NSB.

175. Accordingly, Plaintiff Marchand on behalf of himself and the New Hampshire Subclass, seeks actual damages, injunctive relief, other equitable relief, costs, and attorneys' fees.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs, on behalf of themselves, the Class, and the Subclasses described above, seek the following relief:

1. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class and their respective Subclasses requested herein;
2. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;
3. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;
4. An order instructing Defendants to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;
5. An order requiring Defendants to pay the costs involved in notifying Class Members about the judgment and administering the claims process;
6. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

7. An award of such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: April 1, 2026

Respectfully submitted,

Adam T. Savett

Adam T. Savett

Matthew Insley-Pruitt (*pro hac vice*  
forthcoming)

Justyn J. Millamena (*pro hac vice*  
forthcoming)

WOLF POPPER LLP

570 Lexington Ave., 19<sup>th</sup> Floor

New York, NY 10022

Tel: (212) 759-4600

ASavett@wolfpopper.com

MInsley-Pruitt@wolfpopper.com

JMillamena@wolfpopper.com