Tina Wolfson (SBN 174806)
*twolfson@ahdootwolfson.com*
Bradley K. King (SBN 274399)
*bking@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
10728 Lindbrook Drive
Los Angeles, CA 90024
Tel: (310) 474-9111
Fax: (310) 474-8585

Cornelius P. Dukelow*
Oklahoma Bar No. 19086
**ABINGTON COLE + ELLERY**
320 South Boston Avenue
Suite 1130
Tulsa, Oklahoma 74103
918.588.3400 (*telephone & facsimile*)
cdukelow@abingtonlaw.com

**Pro Hac Vice* application to be submitted

*Counsel for Plaintiff*

**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF CALIFORNIA**

JOSE LOPEZ, individually and on behalf of all others similarly situated,

Plaintiff,

v.

TANDEM DIABETES CARE, INC.,

Defendant.

Case No. **'20CV0723 GPC BGS**

**CLASS ACTION COMPLAINT**

DEMAND FOR JURY TRIAL

Plaintiff, Jose Lopez ("Plaintiff"), individually and on behalf of all others similarly situated, alleges the following against Defendant Tandem Diabetes Care, Inc. ("Defendant" or "Tandem") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

## BRIEF SUMMARY OF THE CASE

1. Defendant is a public US medical device manufacturer that develops medical technologies for the treatment of diabetes.

2. On January 17, 2020, Defendant learned it was experiencing a data breach (the "Data Breach") resulting in the exposure and exfiltration of sensitive personal and medical information of approximately 140,781 patients ("Affected Patients").

3. The Affected Patients' data exposed by Defendant and exfiltrated in the Data Breach included the types of information that federal and state law requires companies to take security measures to protect: names, contact information, Social Security numbers, information related to the use of Defendant's products or services, and clinical data regarding diabetes therapy ("Personal and Medical Information"). This data should have received the most rigorous protection available – it did not.

4. Even though Defendant was storing sensitive Personal and Medical Information that it knew was valuable to criminals, and vulnerable to exfiltration, Defendant failed to take security precautions necessary to protect Affected Patients' data. Because Defendant failed to take necessary security precautions, Affected Patients' Personal and Medical Information was accessed and exfiltrated.

## PARTIES

5. Plaintiff Jose Lopez is an individual residing in Huffman, Texas. Plaintiff Lopez purchased an insulin pump from Defendant in 2019. Defendant received and collected Plaintiff Lopez's Personal and Medical Information, which Defendant maintained in its computer systems. In March 2020, Plaintiff Lopez received a letter dated March 12, 2020, from Defendant informing him that his Personal and Medical Information was

compromised as a result of the Data Breach. Since learning of the Data Breach, Plaintiff Lopez has learned that an insurance policy that is not his and that he knows nothing about has become associated with his Tandem account and he is concerned that this may result in fraudulent insurance claims being made in his name. Since learning of the Data Breach, Plaintiff Lopez has become worried that he will become a victim of identity theft or other fraud, which is causing him stress and anxiety. Since learning of the Data Breach, Plaintiff Lopez has spent in excess of 1 hour of his own time trying to make sure he has not and does not become victimized because of the Data Breach.

6. Defendant Tandem Diabetes Care, Inc. is a Delaware corporation with its principal place of business and headquarters in San Diego, California.

## JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d) because the amount in controversy exceeds $5,000,000 (exclusive of interests and costs), because there are more than 100 members in each of the proposed classes, and because at least one member of each of the proposed classes is a citizen of a State different from Defendant.

8. This Court has personal jurisdiction over Defendant because it is headquartered in California, its principal place of business is in California, and it regularly conducts business in California.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in, was directed to, and/or emanated from this District.

## STATEMENT OF FACTS

### Defendant

10. Defendant is a US medical device company that designs, develops and commercializes products for people with diabetes who use insulin.

11. As part of its business, Defendant receives, collects, and maintains on its computer systems a large amount of sensitive Personal and Medical Information, the

disclosure of which may be personally or professionally damaging for some individuals, and which, when in the possession of unscrupulous individuals, may be used to commit various forms of fraud and identity theft.

**The Data Breach**

12. On March 16, 2020, Defendant, for the first time, publicly admitted via a press release ("Press Release") that it "will be notifying its customers of an information security incident involving five Tandem employee email accounts."[1]

13. The Press Release further stated that "[Defendant] will begin mailing letters to affected customers explaining the incident on March 17, 2020."

14. On March 17, 2020, Defendant began filing with various state Attorneys General sample data breach notification letters that mirrored the language of letters Defendant began mailing to Affected Patients (including Plaintiff and Class Members) on or about that same date. The data breach notification letter Defendant filed with the Attorney General of California on March 17, 2020, is attached hereto as Exhibit 1.

15. According to both the Press Release and the data breach notification letter, Defendant first learned of the Data Breach on January 17, 2020.

16. According to both the Press Release and the data breach notification letter, the Data Breach began on January 17, 2020, and lasted until January 20, 2020. Thus, even though Defendant learned of the data breach on the day it began, it didn't stop the breach until 3 days later.

17. According to the Press Release (and the data breach notification letter in slightly different language), "an unauthorized user gained access to an employee's email account through a 'phishing' incident."

[1] *Tandem Diabetes Care Announces Security Incident with Five Employee Email Accounts* (March 16, 2020), http://investor.tandemdiabetes.com/news-releases/news-release-details/tandem-diabetes-care-announces-security-incident-five-employee (last visited Apr. 15, 2020).

18. According to the Press Release (and the data breach notification letter in slightly different language), after learning of the breach on January 17, 2020, Defendant immediately began investigating and "determined that a limited number of Company employee email accounts may have been accessed by the unauthorized user between January 17, 2020 and January 20, 2020."

19. According to the Press Release, Defendant's "investigation determined that some customer information was contained within these email accounts, including customer contact information, information related to the use of Tandem's products or services, and/or clinical data regarding customer diabetes therapy, and in some very limited instances, customer Social Security numbers."

20. On March 17, 2020, Defendant filed a notice with the U.S. Department of Health and Human Services Office for Civil Rights indicating a "Hacking/IT Incident" of unsecured protected health information of 140,781 individuals.

21. Personal and Medical Information disclosed in the Data Breach included Affected Patients' names, contact information, Social Security numbers, information related to the use of Defendant's products or services, and clinical data regarding diabetes therapy.

22. Affected Patients' Personal and Medical Information described above was exfiltrated during the Data Breach.

23. Defendant's data breach notification letter acknowledged the very real threat that the incident would result in identity theft, fraud, and other similar risks by further informing recipients of the notice – such as Plaintiff and Class Members – to "be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity."

24. Defendant's data breach notification letter advises victims that "[i]f you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state."

25. Defendant's data breach notification letter also explains to victims how to establish fraud alerts with the three credit bureaus and establish credit security freezes.

26. Notably, to date, Defendant has not offered or provided to the victims any fraud insurance. Instead, Defendant merely offered 12 months of credit monitoring services to victims. Defendant made general suggestions to contact local authorities and police, in addition to suggestions on implementing a credit freeze if necessary. Essentially, all these steps are mandated generalities used by virtually every company when publishing alerts about data security breaches. Defendant failed to make any additional effort to mitigate or remediate the damage caused by its failure to protect Affected Patients' Personal and Medical Information.

27. Although Defendant knew of the Data Breach no later than January 17, 2020, Defendant took no steps to notify Affected Patients until March 16, 2020, via Defendant's Press Release, and until on or about March 17, 2020, when Defendant began mailing data breach notification letters to Affected Patients directly. This was a delay of not less than 59-60 days. (The statement in the Press Release that "[Defendant] will begin mailing letters to affected customers explaining the incident on March 17, 2020" suggests at least some data breach notification letters were sent after March 17, 2020.)

**Defendant Expressly Promised to Protect Personal and Medical Information and Acknowledged It is Required by Law to Protect Personal and Medical Information**

28. Defendant's Notice of Privacy Practices[2] states, as relevant:

> Tandem Diabetes Care takes your privacy very seriously.
>
> ***
>
> We take the privacy of your personal data very seriously, and several laws and regulations require us to handle your data in very specific ways. The data privacy principles we follow are:

[2] *Notice of Privacy Practices*, https://www.tandemdiabetes.com/privacy/privacy-policy (last visited Apr. 15, 2020).

- We will transparently explain how we collect, use, and disclose your data in clear, plain language.
- We will collect, use, and disclose your data only for the purposes specified in this Notice, in the Notices listed in the scope of this notice section, and in accordance with any separately-obtained consent. You may request to withdraw your consent at any time.
- We will use commercially reasonable measures to protect your data from loss, theft, and unauthorized access.
- We will collect, use, and disclose your data in a fair, legal way.

***

[W]e place high value on protecting your information, and have implemented appropriate physical, electronic, and administrative procedures to safeguard and secure the personal information we collect from you. By doing that, we seek to protect the confidentiality, integrity, availability, and privacy of your data while keeping your data free from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access.

29. Defendant's Notice of HIPAA Privacy Practices[3] states, as relevant:

Tandem is providing you with this Notice because it is required by the Health Insurance Portability and Accountability Act (HIPAA) and because we are committed to protecting the privacy and security of your personal data. This Notice applies to individuals whose electronic health data we collect, use, or disclose in relation to our diabetes products and services. This Notice is meant to be

[3] *Notice of HIPAA Privacy Practices*, https://www.tandemdiabetes.com/privacy/hippa (last visited Apr. 15, 2020).

> read in addition to, and not in the place of, the information provided in Tandem's Notice of Privacy Practices.
>
> ***
>
> Our Responsibilities
>
> - We are required by law to maintain the privacy and security of your protected health information.
> - We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
> - We must follow the duties and privacy practices described in this Notice and give you a copy of it.
> - We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.

30. Notwithstanding the foregoing assurances, promises, and obligations, Defendant failed to protect the Personal and Medical Information of Plaintiff and other Class Members, as conceded in Defendant's Press Release and in Defendant's data breach notification letters to Affected Patients.

31. If Defendant truly understood the importance of safeguarding Affected Patients' Personal and Medical Information, it would acknowledge its responsibility for the harm it has caused, and would compensate Class Members, provide long-term protection for Plaintiff and Class Members, agree to Court-ordered and enforceable changes to its cybersecurity policies and procedures, and adopt regular and intensive training to ensure that a data breach like this never happens again.

32. Defendant's data security obligations were particularly important given the known substantial increase in data breaches in the healthcare industry, including the recent massive data breaches involving LabCorp, Quest Diagnostics, and American Medical Collections Agency. And given the wide publicity given to these data breaches, there is no

excuse for Defendant's failure to adequately protect Plaintiff and Class Members' Personal and Medical Information.

**Defendant had an Obligation to Protect Personal and Medical Information under Federal and State Law and the Applicable Standard of Care**

33. Defendant had obligations created by HIPAA (42 U.S.C. § 1302d *et. seq.*), California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56 *et seq.*), California's Consumer Records Act (Cal. Civ. Code § 1798.82 *et seq.*) and based on industry standards, to keep the compromised Personal and Medical Information confidential and to protect it from unauthorized disclosures. Plaintiff and Class Members provided their Personal and Medical Information to Defendant with the common sense understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized disclosures.

34. Defendant's data security obligations and promises were particularly important given the substantial increase in data breaches – particularly those in the healthcare industry – which were widely known to the public and to anyone in Defendant's industries.

35. Defendant failed to spend sufficient resources on monitoring external incoming emails and training its employees to identify email-born threats and defend against them.

36. Defendant is an entity covered by HIPAA (45 C.F.R. § 160.102). As such, it is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

37. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

38. HIPAA's Security Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is maintained or transferred in electronic form.

39. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

40. "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.

41. HIPAA's Security Rule requires Defendant to 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.

42. HIPAA also required Defendant 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).

43. HIPAA also required Defendant 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).

44. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[4]

45. Defendant's security failures demonstrate that it failed to honor its duties and promises by not:

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

b. Adequately protecting Plaintiff's and Class Members' Personal and Medical Information;

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

d. Implementing 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 in violation of 45 C.F.R. § 164.312(a)(1);

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

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

g. Protecting against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2);

[4] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited Apr. 15, 2020).

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

i. Ensuring compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4); and/or

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

46. Defendant was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

47. As described before, Defendant is also required (by the CCRA, CMIA and various other states' laws and regulations) to protect Plaintiff's and Class Members' Personal and Medical Information, and further, to handle any breach of the same in accordance with applicable breach notification statutes.

48. In addition to its obligations under federal and state laws, Defendant owed a duty to Affected Patients whose Personal and Medical Information was entrusted to Defendant to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal and Medical Information in its possession from being compromised, lost, stolen, accessed, and/or misused by unauthorized persons. Defendant owed a duty to Affected Patients to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems and networks,

and the personnel responsible for them, adequately protected the Personal and Medical Information of the Affected Patients.

49. Defendant owed a duty to Affected Patients whose Personal and Medical Information was entrusted to Defendant to design, maintain, and test its computer systems to ensure that the Personal and Medical Information in Defendant's possession was adequately secured and protected.

50. Defendant owed a duty to Affected Patients whose Personal and Medical Information was entrusted to Defendant to create and implement reasonable data security practices and procedures to protect the Personal and Medical Information in its possession, including adequately training its employees and others who accessed Personal and Medical Information within its computer systems on how to adequately protect Personal and Medical Information.

51. Defendant owed a duty to Affected Patients whose Personal and Medical Information was entrusted to Defendant to implement processes that would detect a breach on its data security systems in a timely manner.

52. Defendant owed a duty to Affected Patients whose Personal and Medical Information was entrusted to Defendant to act upon data security warnings and alerts in a timely fashion.

53. Defendant owed a duty to Affected Patients whose Personal and Medical Information was entrusted to Defendant to adequately train and supervise its employees to identify and avoid any phishing emails that make it past its email filtering service.

54. Defendant owed a duty to Affected Patients whose Personal and Medical Information was entrusted to Defendant to adequately train and supervise its employees to detect a breach on its data security systems in a timely manner.

55. Defendant owed a duty to Affected Patients whose Personal and Medical Information was entrusted to Defendant to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Personal and Medical Information from

exfiltration because such an inadequacy would be a material fact in the decision to entrust Personal and Medical Information with Defendant.

56. Defendant owed a duty to Affected Patients whose Personal and Medical Information was entrusted to Defendant to disclose in a timely and accurate manner when data breaches occurred.

57. Defendant owed a duty of care to Affected Patients because they were foreseeable and probable victims of any inadequate data security practices.

**Defendant Was on Notice of Data Breach Threats and the Inadequacy of Its Data Security**

58. Defendant was on notice that companies in the healthcare industry were targets for cyberattacks.

59. Defendant was on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[5]

60. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only

[5] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited Apr. 15, 2020).

threaten the privacy and security of patients' health and financial information, but also patient access to care.[6]

61. As implied by the above quote from the AMA, stolen Personal and Medical Information can be used to interrupt important medical services themselves. This is an imminent and certainly impending risk for all Affected Patients.

62. Defendant was on notice that the federal government has been concerned about healthcare company data encryption. Defendant knew it kept protected health information in its computer systems and email accounts and yet did not encrypt its computer systems and email accounts.

63. The United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, the DHHS's Office of Human Rights' deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[7]

64. As a covered entity or business associate under HIPAA, Defendant should have known about its weakness toward email-related data security threats and sought better protection for the Personal and Medical Information in its computer systems and employee email accounts.

---

[6] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Apr. 15, 2020).

[7] *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20150618190135/http://www.hhs.gov/news/press/2014pres/04/20140422b.html (last visited Apr. 15, 2020).

65. In the healthcare industry, the number one threat vector from a cyber security standpoint is phishing. Cybersecurity firm Proofpoint reports that "phishing is the initial point of compromise in most significant [healthcare] security incidents, according to a recent report from the Healthcare Information and Management Systems Society (HIMSS). And yet, 18% of healthcare organizations fail to conduct phishing tests, a finding HIMSS describes as 'incredible.'"[8]

66. The report from Proofpoint was published March 27, 2019, and summarized findings of recent healthcare industry cyber threat surveys and recounted good, common sense steps that the targeted healthcare companies should follow to prevent email-related cyberattacks.

67. One of the best protections against email related threats is security awareness training and testing on a regular basis. This should be a key part of a company's on-going training of its employees. "[S]ince phishing is still a significant, initial point of compromise, additional work needs to be done to further lower the click rate," the HIMSS report states. "This can be done through more frequent security awareness training, phishing simulation, and better monitoring of metrics pertaining to phishing (including whether there are any particular repeat offenders)."[9]

68. ProtonMail Technologies publishes a guide for IT Security to small businesses (i.e., companies without the heightened standard of care applicable in the healthcare industry). In its 2019 guide, ProtonMail dedicates a full chapter of its ebook guide to the danger of phishing and ways to prevent a small business from falling prey to it. It reports:

> Phishing and fraud are becoming ever more extensive problems. A recent threat survey from the cybersecurity firm Proofpoint stated that between 2017 and 2018, email-based attacks on businesses

[8] Aaron Jensen, Healthcare Phishing Statistics: 2019 HIMSS Survey Results (Mar. 27, 2019), https://www.proofpoint.com/us/security-awareness/post/healthcare-phishing-statistics-2019-himss-survey-results (last visited Apr. 15, 2020).

[9] *Id.*

> increased 476 percent. The FBI reported that these types of attacks cost companies around the world $12 billion annually.
>
> Similar to your overall IT security, your email security relies on training your employees to implement security best practices and to recognize possible phishing attempts. This must be deeply ingrained into every staff member so that every time they check their emails, they are alert to the possibility of malicious action.[10]

69. The guidance that ProtonMail provides non-healthcare industry small businesses is likely still not adequate for a company like Defendant, with the heightened healthcare standard of care based on HIPAA, CMIA, and the increased danger from the sensitivity and wealth of Personal and Medical Information it retains, but ProtonMail's guidance is informative for showing how inadequately Defendant protected the Personal and Medical Information of the Plaintiffs and Class Members. ProofPoint lists numerous tools under the heading, "How to Prevent Phishing":

a. **Training:** "Training your employees on how to recognize phishing emails and what to do when they encounter one is the first and most important step in maintaining email security. *This training should be continuous as well. . . .*"

b. **Limit Public Information:** "Attackers cannot target your employees if they don't know their email addresses. Don't publish non-essential contact details on your website or any public directories . . . .

c. **Carefully check emails:** "First off, your employees should be skeptical anytime they receive an email from an unknown sender. Second, most phishing emails are riddled with typos, odd syntax, or stilted language.

[10] *The ProtonMail Guide to IT Security for Small Businesses*, ProtonMail (2019), available at https://protonmail.com/it-security-complete-guide-for-businesses (last visited Apr. 15, 2020).

Finally, check the 'From' address to see if it is odd . . . . If an email looks suspicious, employees should report it."

d. **Beware of links and attachments:** "Do not click on links or download attachments without verifying the source first and establishing the legitimacy of the link or attachment. . . ."

e. **Do not automatically download remote content:** "Remote content in emails, like photos, can run scripts on your computer that you are not expecting, and advanced hackers can hide malicious code in them. You should configure your email service provider to not automatically download remote content. This will allow you to verify an email is legitimate before you run any unknown scripts contained in it."

f. **Hover over hyperlinks:** "Never click on hyperlinked text without hovering your cursor over the link first to check the destination URL, which should appear in the lower corner of your window. Sometimes the hacker might disguise a malicious link as a short URL." [Proofpoint notes that there are tools online available for retrieving original URLs from shortened ones.]

g. **If in doubt, investigate:** "Often phishing emails will try to create a false sense of urgency by saying something requires your immediate action. However, if your employees are not sure if an email is genuine, they should not be afraid to take extra time to verify the email. This might include asking a colleague, your IT security lead, looking up the website of the service the email is purportedly from, or, if they have a phone number, calling the institution, colleague, or client that sent the email."

h. **Take preventative measures:** "Using an end-to-end encrypted email service gives your business's emails an added layer of protection in the case of a data breach. A spam filter will remove the numerous random emails that you might receive, making it more difficult for a phishing attack to get through. Finally, other tools, like Domain-based Message Authentication, Reporting,

and Conformance (DMARC) help you be sure that the email came from the person it claims to come from, making it easier to identify potential phishing attacks."[11]

70. These are basic, common-sense email security measures that ever business, not even healthcare businesses, should be doing. Defendant, with its heightened standard of care should be doing even more. But by adequately taking these common-sense solutions, Defendant could have prevented this Data Breach from occurring.

**It is Well Established That Data Breaches Lead to Identity Theft and Other Harms**

71. Plaintiff and Class Members have been injured by the disclosure and exfiltration of their Personal and Medical Information in the Data Breach.

72. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[12] Cyber criminals can leverage Plaintiff's and Class Members' Personal and Medical Information that was exfiltrated in the Data Breach to commit thousands of crimes, including opening new financial accounts in Affected Patients' names, taking out loans in Affected Patients' names, using Affected Patients' names to obtain medical services, using Affected Patients' Personal Information to file fraudulent tax returns, using Affected Patients' health insurance information to rack up medical debts in their names, using Affected Patients' health information to target them in other phishing and hacking intrusions based on their individual health needs, using Affected Patients' information to obtain government benefits, obtaining driver's licenses in Affected Patients' names but with another person's photograph, and giving false information to police during an arrest. Even worse, Affected Patients could be arrested for crimes identity thieves have committed.

[11] *Id.*

[12] *Facts + Statistics: Identity Theft and Cybercrime*, Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last visited Apr. 15, 2020).

73. Personal and Medical Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black-market for years.

74. This is not just speculative. As the FTC has reported, if hackers get access to Personal and Medical Information, they ***will*** use it.[13]

75. For instance, with a stolen social security number, which is part of the Personal and Medical Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[14] Identity thieves can also use the information stolen from Breach Victims to qualify for expensive medical care and leave them and their contracted health insurers on the hook for massive medical bills.

76. Medical identity theft is one of the most common, most expensive, and most difficult to prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more "than identity thefts involving banking and finance, the government and the military, or education."[15]

77. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they

[13] Ari Lazarus, *How fast will identity thieves use stolen info?*, Fed. Trade Comm'n (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info (last visited Apr. 15, 2020).

[14] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited Apr. 15, 2020).

[15] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last visited Apr. 15, 2020).

frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[16]

78. 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 can go from $20 say up to – we've seen $60 or $70 [(referring to prices on dark web marketplaces)]."[17] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[18]

79. If, moreover, cyber criminals also manage to acquire financial information, credit and debit cards, health insurance information, driver's licenses and passports, there is no limit to the amount of fraud to which Defendant has exposed the Affected Patients.

80. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and credit in a person's name.[19] As the GAO Report states, this type of identity theft

---

[16] *Id.*

[17] IDExperts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited Apr. 15, 2020).

[18] *Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS: Key findings from The Global State of Information Security Survey 2015, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Apr. 15, 2020).

[19] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 15, 2020).

is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

81. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[20]

82. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

83. There may be a time lag between when sensitive personal information is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, ***stolen data may be held for up to a year or more before being used to commit identity theft***. Further, once stolen data have been sold or posted on the Web, ***fraudulent use of that information may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[21]

84. With access to an individual's Personal and Medical Information, criminals can do more than just empty a victim's bank account – they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's

[20] *Id.* at 2, 9.

[21] *Id.* at 29 (emphasis added).

name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[22]

85. Personal and Medical Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other Personal and Medical Information directly on various Internet websites making the information publicly available.

86. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[23] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

87. Medical computer systems are especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value – whereas a stolen social security number, on the other hand, only sells for $1."[24] In fact, the medical industry has experienced disproportionally higher instances of computer theft than any other industry.

---

[22] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Apr. 15, 2020).

[23] *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 Apr. 15, 2020).

[24] Study: Few Aware of Medical Identity Theft Risk, Claims Journal, https://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited Apr. 15, 2020).

88. Furthermore, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[25]

89. To date, other than providing 12 months of credit monitoring, Defendant does not appear to be taking any measures to assist Plaintiff and Class Members other than telling them to simply do the following:

- "be vigilant for incidents of fraud or identity theft";
- "review[] your account statements and free credit reports for any unauthorized activity";
- obtain a copy of free credit reports;
- contact the FTC and/or the state Attorney General's office;
- enact a security freeze on credit files; and
- create a fraud alert.

None of these recommendations, however, require Defendant to expend any effort to protect Plaintiff's and Class Members' Personal and Medical Information.

90. Defendant's failure to adequately protect Plaintiff's and Class Members' Personal and Medical Information has resulted in Plaintiff and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money – while Defendant sits by and does nothing to assist those affected by the incident. Instead, as Defendant's notice indicates, it is putting the burden on the Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

91. Defendant's offer of 12 months of identity monitoring to Plaintiff and Class Members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered,

[25] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last visited Apr. 15, 2020).

and also between when Personal and Medical Information is acquired and when it is used. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's Personal and Medical Information) – it does not prevent identity theft.[26] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

92. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class Members must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

93. Plaintiff and the Class Members have suffered, continue to suffer and/or will suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including Personal and Medical Information;

b. Improper disclosure of their Personal and Medical Information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal and Medical Information being placed in the hands of criminals;

d. The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

[26] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited Apr. 15, 2020).

e. Damages flowing from Defendant's untimely and inadequate notification of the data breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of Affected Patients' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Personal and Medical Information; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

94. Moreover, Plaintiff and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards.

95. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiff and Class Members 12 months of identity theft monitoring services. 12 months of identity theft monitoring is woefully inadequate to protect Plaintiff and Class Members from a lifetime of identity theft risk and does nothing to reimburse Plaintiff and Class Members for the injuries they have already suffered.

## CHOICE OF LAW

96. The State of California has a significant interest in regulating the conduct of businesses operating within its borders. California seeks to protect the rights and interests of all California residents and citizens of the United States against a company headquartered and doing business in California. California has a greater interest in the nationwide claims of

Plaintiff and members of the Nationwide Class than any other state and is most intimately concerned with the claims and outcome of this litigation.

97. The corporate headquarters of Defendant, located in San Diego, California, is the "nerve center" of its business activities – the place where its officers direct, control, and coordinate the company's activities, including its data security functions and policy, financial, and legal decisions.

98. Defendant's response to the Data Breach at issue here, and corporate decisions surrounding such response, were made from and in California.

99. Defendant's breaches of duty to Plaintiff and Nationwide Class members emanated from California.

100. Application of California law to the Nationwide Class with respect to Plaintiff's and Class Members' claims is neither arbitrary nor fundamentally unfair because California has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiff and the Nationwide Class.

101. Under California's choice of law principles, which are applicable to this action, the common law of California applies to the nationwide common law claims of all Nationwide Class members. Additionally, given California's significant interest in regulating the conduct of businesses operating within its borders, California's Unfair Competition Law and Confidentiality of Medical Information Act may be applied to non-resident plaintiffs as against this resident defendant.

## CLASS ALLEGATIONS

102. Plaintiff brings this class action lawsuit individually and on behalf of the proposed Class Members under Rule 23 of the Federal Rules of Civil Procedure.

103. Plaintiff seeks certification of a Nationwide Class and a Texas Sub-Class defined as follows:

> Nationwide Class: All persons in the United States whose Personal and Medical Information was compromised as a result of the

Tandem Data Breach announced by Tandem on or around March 16, 2020.

104. In the alternative to the Nationwide Class, Plaintiff seeks certification of the following Texas state class:

Texas Sub-Class: All persons in the State of Texas whose Personal and Medical Information was compromised as a result of the Tandem Data Breach announced by Tandem on or around March 16, 2020.

105. Specifically excluded from the Classes are Defendant and any entities in which Defendant has a controlling interest, Defendant's agents and employees, the judge to whom this action is assigned, members of the judge's staff, and the judge's immediate family.

106. **Numerosity:** Plaintiff does not know the exact number of Class Members, but believes the Classes comprise approximately 140,000 individuals throughout the United States. As such, Class Members are so numerous that joinder of all members is impracticable.

107. **Commonality:** Common questions of law and fact exist and predominate over any questions affecting only individual Class Members. The common questions include:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and Class Members' Personal and Medical Information;

c. Whether Defendant failed to protect Plaintiff's and Class Members' Personal and Medical Information properly and/or as promised;

d. Whether Defendant's computer system and data security practices used to protect Plaintiff's and the Class Members' Personal and Medical Information violated federal, state or local laws, or Defendant's duties;

e. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Personal and Medical Information;

f. Whether Defendant violated the consumer protection statutes, data breach notification statutes, state unfair insurance practice statutes, state insurance privacy statutes, and/or state medical privacy statutes applicable to Plaintiff and Class Members;

g. Whether Defendant failed to notify Plaintiff and Class Members about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

h. Whether Defendant acted negligently in failing to safeguard Plaintiff's and Class Members' Personal and Medical Information;

i. Whether Defendant express or implied contractual obligations to protect the confidentiality of Plaintiff's and the Class Members' Personal and Medical Information, and to have reasonable data security measures;

j. Whether Defendant's conduct described herein constitutes a breach of contract with Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

m. What equitable relief is appropriate to redress Defendant's wrongful conduct; and

n. What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Plaintiff and Class Members.

108. **Typicality:** Plaintiff's claims are typical of the claims of the Class Members. Plaintiff and Class Members were injured through Defendant's uniform misconduct and their legal claims arise from the same core practices of Defendant.

109. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Classes and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Classes, and there are no defenses unique to Plaintiff. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Classes and

have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Classes.

110. **Risks:** The proposed action meets the requirements of Fed. R. Civ. P. 23 because prosecution of separate actions by individual members of the Classes would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Defendant or would be dispositive of the interests of members of the proposed Classes. Furthermore, Defendant's computer system still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of Defendant's computer system.

111. **Injunctive Relief:** The proposed action meets the requirements of Fed. R. Civ. P. 23(b)(2) because Defendant has acted or has refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

112. **Predominance:** The proposed action meets the requirements of Fed. R. Civ. P. 23(b)(3) because questions of law and fact common to the Classes predominate over any questions that may affect only individual Class Members in the proposed Classes.

113. **Superiority:** The proposed action also meets the requirements of Fed. R. Civ. P. 23(b)(3) because a class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class Member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Defendant. Even if it were economically feasible, requiring approximately 140,000 injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. Plaintiff anticipates no unusual difficulties in managing this class action.

114. **Certification of Particular Issues:** In the alternative, this action may be maintained as class action with respect to particular issues in accordance with Fed. R. Civ. P. 23(c)(4).

115. Finally, all members of the purposed Classes are readily ascertainable. Defendant has access to addresses and other contact information for members of the Classes, which can be used to identify Class Members.

## COUNT I

## NEGLIGENCE

116. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

117. This count is brought on behalf of all Classes.

118. Defendant collected and stored the Personal and Medical Information of Plaintiff and Class Members.

119. Defendant knew, or should have known, of the risks inherent in collecting and storing the Personal and Medical Information of Plaintiff and Class Members.

120. Defendant owed duties of care to Plaintiff and Class Members whose Personal and Medical Information had been entrusted with Defendant.

121. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Personal and Medical Information.

122. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' Personal and Medical Information. Defendant knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known that hackers were attempting to access the Personal and Medical Information in health care computer systems, such as theirs.

123. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Defendant entered into a "special relationship" with Plaintiff and Class Members by placing their Personal and Medical Information in Defendant's computer system – information that Plaintiff and Class Members had been required to provide to Defendant.

124. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

125. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Personal and Medical Information.

126. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members now face an increased risk of future harm.

127. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

## COUNT II

## NEGLIGENCE *PER SE*

128. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

129. This count is brought on behalf of all Classes.

130. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Personal and Medical Information.

131. Pursuant to HIPAA (42 U.S.C. § 1302d *et. seq.*), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Personal and Medical Information.

132. Pursuant to Cal. Civ. Code § 56 *et seq.*, Defendant had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' Personal and Medical Information.

133. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et. seq.*), and Cal. Civ. Code § 56 *et seq.* by failing to provide fair, reasonable, or adequate computer systems and

data security practices to safeguard Plaintiff's and Class Members' Personal and Medical Information.

134. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

135. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

136. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Personal and Medical Information.

137. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members now face an increased risk of future harm.

138. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

## COUNT III

## BREACH OF CONTRACT

139. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

140. This count is brought on behalf of all Classes.

141. As the operator of healthcare facilities, Defendant entered into contracts with Plaintiff and Class Members.

142. The promises and representations described above relating to HIPAA, CMIA, and industry practices, and about Defendant's purported concern about its patients' privacy rights became terms of the contract between it and its customers, including Plaintiff and Class Members.

143. Defendant breached these promises by failing to comply with HIPAA, CMIA, and reasonable industry practices.

144. As a result of Defendant's breach of these terms, Plaintiff and Class Members have been harmed and put at risk of future harm.

145. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

## COUNT IV

## BREACH OF IMPLIED CONTRACT

146. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

147. This count is brought on behalf of all Classes.

148. When Plaintiff and the Class Members provided their Personal and Medical Information to Defendant when seeking treatment, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect their Personal and Medical Information and to timely notify them in the event of a data breach.

149. Defendant required its patients (including Plaintiff and Class Members) to provide Personal and Medical Information in order to receive treatment from Defendant.

150. Defendant affirmatively represented that it collected and stored the Personal and Medical Information of Plaintiff and Class Members in compliance with HIPAA, the CMIA, and other statutory and common law duties, and using reasonable, industry standard means.

151. Based on the implicit understanding and on Defendant's representations (as described above), Plaintiff and Class Members accepted Defendant's offers and provided Defendant with their Personal and Medical Information.

152. Plaintiff and Class Members would not have provided their Personal and Medical Information to Defendant had they known that Defendant would not safeguard their Personal and Medical Information as promised or provide timely notice of a data breach.

153. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

154. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' personal information and failing to provide them with timely and accurate notice of the Data Breach.

155. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of the implied contract with Plaintiff and Class Members.

## COUNT V

## BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

156. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

157. This count is brought on behalf of all Classes.

158. As described above, Defendant made promises and representations to Plaintiff and Class Members that it would comply with HIPAA, the CMIA and other applicable laws and industry best practices.

159. These promises and representations became a part of the contract between Defendant and Plaintiff and Class Members.

160. While Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

161. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations (including California's UCL), and when it engaged in unlawful practices under HIPAA, the CMIA, and other laws. These acts and omissions included: representing that it would maintain adequate data privacy and security practices and procedures to safeguard the Personal and Medical Information from unauthorized disclosures, releases, data breaches, and theft; omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class Members' Personal and Medical Information; and failing to disclose to Plaintiff and Class Members at the time they provided

their Personal and Medical Information to it that Defendant's data security systems, including training, auditing, and testing of employees, failed to meet applicable legal and industry standards.

162. Plaintiff and Class Members did all or substantially all the significant things that the contract required them to do.

163. Likewise, all conditions required for Defendant's performance were met.

164. Defendant's acts and omissions unfairly interfered with Plaintiff's and Class Members' rights to receive the full benefit of their contracts.

165. Plaintiff and Class Members have been harmed by Defendant's breach of this implied covenant in the many ways described above, including overpayment for products and services, actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their Personal and Medical Information, and the attendant long-term expense of attempting to mitigate and insure against these risks.

166. Defendant is liable for this breach of these implied covenants whether or not it is found to have breached any specific express contractual term.

167. Plaintiff and Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

## COUNT VI

## UNJUST ENRICHMENT

168. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

169. This count is brought on behalf of all Classes.

170. Plaintiff and Class Members conferred a monetary benefit on Defendant. Defendant received and retained money belonging to Plaintiff and Class Members either directly through copayments and coinsurance or indirectly through health insurance/medical plans they had paid for.

171. Defendant had knowledge of the benefits conferred on it by Plaintiff and the Class Members.

172. The money that Plaintiff and Class Members paid to Defendant was supposed to be used by Defendant, in part, to pay for the costs of HIPAA and CMIA compliance and reasonable data privacy and security practices and procedures.

173. As a result of Defendant's conduct, Plaintiff and Class Members suffered damages in an amount equal to the difference in value between health care services with the reasonable data privacy and security practices and procedures that they paid for, and the inadequate health care services without reasonable data privacy and security practices and procedures that they received.

174. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement (or to adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated by HIPAA regulations, federal, state, and local laws, and industry standards.

175. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds that Defendant received.

176. A constructive trust should be imposed on all unlawful or inequitable sums received by Defendant traceable to Plaintiff and Class Members.

## COUNT VII

## VIOLATIONS OF CALIFORNIA'S UNFAIR COMPETITION LAW

## Cal. Bus. & Prof. Code §17200, *et seq.*

177. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

178. This count is brought on behalf of all Classes.

179. Defendant is headquartered in California. Defendant violated California's Unfair Competition Law ("UCL"), Cal. Bus. Prof. Code § 17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or

misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a. by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class Members' Personal and Medical Information from unauthorized disclosure, release, data breach, and theft; representing and advertising that it did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Class Members' Personal and Medical Information; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class Members' Personal and Medical Information;

b. by soliciting and collecting Plaintiff's and Class Members' Personal and Medical Information with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class members' Personal and Medical Information in an unsecure electronic environment;

c. by failing to disclose the Data Breach in a timely and accurate manner, in violation of Cal. Civ. Code §1798.82;

d. by violating the privacy and security requirements of HIPAA, 42 U.S.C. §1302d, *et seq.*;

e. by violating the CMIA, Cal. Civ. Code § 56, *et seq.*; and

f. by violating the CCRA, Cal. Civ. Code § 1798.82.

180. These unfair acts and practices were immortal, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class Members. Defendant's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, et seq., CMIA, Cal. Civ. Code § 56, et seq., and the CCRA, Cal. Civ. Code § 1798.81.5.

181. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiff and Class Members were injured and lost money or property, including but not limited to the overpayments Defendant received to take reasonable and adequate security measures (but did not), the loss of their legally protected interest in the confidentiality and privacy of their Personal and Medical Information, and additional losses described above.

182. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Class Members' Personal and Medical Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class Members.

183. The conduct and practices described above emanated from California where decisions related to Defendant's advertising and data security were made.

184. Plaintiff seeks relief under the UCL, including restitution to Class Members of money or property that the Defendant may have acquired by means of Defendant's deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. P. § 1021.5), and injunctive or other equitable relief.

## COUNT VIII

## VIOLATIONS OF CALIFORNIA'S CONSUMER RECORDS ACT

### Cal. Civ. Code § 1798.82, *et seq.*

185. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

186. This count is brought on behalf of all Classes.

187. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have

been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay . . . ."

188. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

189. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

i. The name and contact information of the reporting person or business subject to this section;

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

iii. If the information is possible to determine at the time the notice is provided, then any of the following:

1. The date of the breach;

2. The estimated date of the breach; or

3. The date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

vi. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

190. The Data Breach described herein constituted a "breach of the security system" of Defendant.

191. As alleged above, Defendant unreasonably delayed informing Plaintiff and Class Members about the Data Breach, affecting their Personal and Medical Information, after Defendant knew the Data Breach had occurred.

192. Defendant failed to disclose to Plaintiff and Class Members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Personal and Medical Information when Defendant knew or reasonably believed such information had been compromised.

193. Defendant's ongoing business interests gave Defendant incentive to conceal the Data Breach from the public to ensure continued revenue.

194. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to Plaintiff and the Class Members would impede its investigation.

195. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff and Class Members because their stolen information would have had less value to identity thieves.

196. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

197. Plaintiff and Class Members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to the damages suffered by Plaintiff and the other Class Members as alleged above and equitable relief.

198. Defendant's misconduct as alleged herein is fraud under Cal. Civ. Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendant conducted with the intent on the part of Defendant of depriving Plaintiff and Class Members of "legal rights or otherwise causing injury." In addition, Defendant's misconduct as alleged herein is malice or oppression under Cal. Civ. Code § 3294(c)(1) and (c)(2) in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiff and Class Members and despicable conduct that has subjected Plaintiff and Class Members to hardship in conscious disregard of their rights. As a result, Plaintiff and Class Members are entitled to punitive damages against Defendant under Cal. Civ. Code § 3294(a).

## COUNT IX

## VIOLATIONS OF CALIFORNIA'S CONFIDENTIALITY OF MEDICAL INFORMATION ACT, Cal. Civ. Code § 56 *et seq.*

199. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

200. This count is brought on behalf of all Classes.

201. Defendant is a "Contractor" as defined by Cal. Civ. Code § 56.05(d) and/or a "Provider of Health Care" as expressed in Cal. Civ. Code § 56.06.

202. Plaintiff and Class Members are "Patients" as defined by Cal. Civ. Code § 56.05(k).

203. The Plaintiff's and Class Members' Personal and Medical Information that was the subject of the Data Breach included "Medical Information" as defined by Cal. Civ. Code § 56.05(j).

204. In violation of California's Confidentiality of Medical Information Act ("CMIA"), Defendant disclosed Medical Information of Plaintiff and Class Members without first obtaining an authorization.

205. In violation of the CMIA, Defendant intentionally shared, sold, used for marketing, or otherwise used Medical Information of Plaintiff and Class Members for a purpose not necessary to provide health care services to Plaintiff or Class Members.

206. In violation of the CMIA, Defendant further disclosed Medical Information regarding Plaintiff and Class Members to persons or entities not engaged in providing direct health care services to Plaintiff or Class Members or their providers of health care or health care service plans or insurers or self-insured employers.

207. In violation of the CMIA, Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of Medical Information of Plaintiff and Class Members in a manner that did not preserve the confidentiality of the information contained therein.

208. In violation of the CMIA, Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Medical Information of Plaintiff and Class Members.

209. In violation of the CMIA, Defendant's electronic health record systems or electronic medical record systems did not protect and preserve the integrity of Plaintiff's and Class Members' Medical Information.

210. In violation of the CMIA, Defendant negligently released confidential information and records of Plaintiff and Class Members.

211. In violation of the CMIA, Defendant negligently disclosed Medical Information of Plaintiff and Class Members.

212. In violation of the CMIA, Defendant knowingly and willfully obtained, disclosed, and/or used Medical Information of Plaintiff and Class Members.

213. As a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56 *et seq*., Plaintiff and Class Members now face an increased risk of future harm.

214. As a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56 *et seq*., Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

## COUNT X

## VIOLATIONS OF CALIFORNIA'S CONSUMER PRIVACY ACT

## Cal. Civ. Code § 1798.100, *et seq.*

215. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

216. This count is brought in the alternative to Plaintiff's CMIA count.

217. This count is brought on behalf of all Classes.

218. Through the above-detailed conduct, Defendant violated California's Consumer Privacy Act ("CCPA") by subjecting the nonencrypted and nonredacted Personal and Medical Information of Plaintiff and Class members to unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature and protection of that information. Cal. Civ. Code § 1798.150(a).

219. In accordance with Cal. Civ. Code § 1798.150(b), prior to the filing of this Complaint, Plaintiff's counsel served Defendant with notice of these CCPA violations by certified mail, return receipt requested.

220. On behalf of Class members, Plaintiff seeks injunctive relief in the form of an order enjoining Defendant from continuing to violate the CCPA. If Defendant fails to respond to Plaintiff's notice letter or agree to rectify the violations detailed above, Plaintiff also will seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any other relief the Court deems proper as a result of Defendant's CCPA violations.

## COUNT XI

## INJUNCTIVE / DECLARATORY RELIEF

221. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

222. This count is brought on behalf of all Classes.

223. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

224. As previously alleged, Plaintiff and Class Members entered into an implied contract that required Defendant to provide adequate security for the Personal and Medical Information it collected from Plaintiff and Class Members.

225. Defendant owes a duty of care to Plaintiff and Class Members requiring it to adequately secure Personal and Medical Information.

226. Defendant still possess Personal and Medical Information regarding Plaintiff and Class Members.

227. Since the Data Breach, Defendant has announced few if any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent further attacks.

228. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the Personal and Medical Information in Defendant's possession is even more vulnerable to cyberattack.

229. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their Personal and Medical Information and Defendant's failure to address the security failings that lead to such exposure.

230. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

231. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

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

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

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

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

e. Ordering that Defendant not transmit Personal and Medical Information via unencrypted email;

f. Ordering that Defendant not store Personal and Medical Information in email accounts;

g. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

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

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

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

## PRAYER FOR RELIEF

Plaintiff, on behalf of himself and the Classes, respectfully requests the Court order relief and enter judgment in their favor and against Tandem as follows:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Classes requested herein.

B. Plaintiff requests injunctive and other equitable relief as is necessary to protect the interests of the Classes, including (i) an order prohibiting Defendant from engaging in the wrongful and unlawful acts described herein; (ii) requiring Defendant to protect all data collected or received through the course of its business in accordance with HIPAA regulations, the CMIA, the CCRA, other federal, state and local laws, and best practices under industry standards; (iii) requiring Defendant to design, maintain, and test its computer systems to ensure that Personal and Medical Information in its possession is adequately secured and protected; (iv) requiring Defendant to disclose any future data breaches in a timely and accurate manner; (v) requiring Defendant to engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis and ordering it to promptly correct any problems or issues detected by these auditors; (vi) requiring Defendant to audit, test, and train its security personnel to run automated security monitoring, aggregating, filtering and reporting on log information in a unified manner; (vii) requiring Defendant to implement multi-factor authentication requirements; (viii) requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; (ix) requiring Defendant to encrypt all Personal and Medical Information; (x) requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures; (xi) requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems; (xii) requiring Defendant to purge, delete, and destroy in a reasonably secure and timely manner Personal and Medical Information no longer necessary for the provision of services; (xiii) requiring Defendant to conduct regular computer system scanning and security checks; (xiv) requiring Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (xv) requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class Members; and (xvi) requiring

Defendant to educate all Class Members about the threats they face as a result of the loss of their Personal and Medical Information to third parties, as well as steps Class Members must take to protect themselves.

C. A judgment awarding Plaintiff and Class Members appropriate monetary relief, including actual damages, punitive damages, treble damages, statutory damages, exemplary damages, equitable relief, restitution, and disgorgement;

D. An order that Defendant pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

E. Pre-judgment and post-judgment interest;

F. Attorneys' fees, expenses, and the costs of this action; and

G. All other and further relief as this Court deems necessary, just, and proper.

**JURY DEMAND**

Plaintiff demands a trial by jury on all issues so triable.

Respectfully submitted,

DATED: April 16, 2020

*/s/ Tina Wolfson*

Tina Wolfson
Bradley K. King
**AHDOOT & WOLFSON, PC**
10728 Lindbrook Drive
Los Angeles, CA 90024
Tel: (310) 474-9111; Fax: (310) 474-8585

Cornelius P. Dukelow*
**ABINGTON COLE + ELLERY**
320 South Boston Avenue
Suite 1130
Tulsa, Oklahoma 74103
918.588.3400 (*telephone & facsimile*)
cdukelow@abingtonlaw.com

**Pro Hac Vice* application to be submitted

*Counsel for Plaintiff*