BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
PAULA R. BROWN (254142)
JENNIFER L. MACPHERSON (202021)
501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
pbrown@bholaw.com
jmacpherson@bholaw.com

BARNOW AND ASSOCIATES, P.C.
BEN BARNOW
ERICH P. SCHORK
ANTHONY L. PARKHILL
205 W. Randolph Street, Suite 1630
Chicago, IL 60602
Tel: 312/621-2000
312/641-5504 (fax)
b.barnow@barnowlaw.com
e.schork@barnowlaw.com
aparkhill@barnowlaw.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

SAMANTHA HENRICHSEN, and her minor son, A.R., individually, and on behalf of all others similarly situated,

Plaintiffs,

v.

TANDEM DIABETES CARE, INC., a Delaware corporation,

Defendant.

Case No. '20CV0732 JM WVG

CLASS ACTION

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff, SAMANTHA HENRICHSEN, and her minor son, A.R., ("Plaintiffs"), individually and on behalf of the general public and all others similarly situated (the "Class members"), by and through their attorneys, upon personal knowledge as to facts pertaining to themselves and on information and belief as to all other matters, bring this class action against Defendant, Tandem Diabetes Care, Inc. ("Tandem"), and respectfully state the following:

NATURE OF THE CASE

1. Tandem is a medical device company that designs, manufactures, sells, and supports products for people with insulin-dependent diabetes including insulin pumps, cartridges, and other related products. As part of its business, Tandem stores and transmits a substantial amount of confidential and personal health information from its customers and their health care providers.

2. On March 16, 2020, Tandem announced that personally identifiably information ("PII") and protected health information ("PHI") (collectively, "PII/PHI") of approximately 140,000 of its patient customers may have been exposed in a phishing attack between January 17 and January 20, 2020. PII/PHI exposed in the breach included customer contact information, customer use of Tandem's products and services, and clinical data regarding customer diabetes therapy, and in some limited instances customer Social Security numbers (the "Data Breach").[1] Although Defendant knew of the breach in early January 2020, or before, it waited almost three months to notify its customers.

3. Defendant owed a duty to Plaintiffs and Class members to maintain reasonable and adequate security measures to secure, protect, and safeguard the PII/PHI it collected and stored on its network. Defendant breached that duty by, *inter alia*, failing to implement and maintain reasonable security procedures and practices

[1] *See* http://investor.tandemdiabetes.com/news-releases/news-release-details/tandem-diabetes-care-announces-security-incident-five-employee.

to protect the PII/PHI from unauthorized access and unnecessarily storing and retaining Plaintiffs' and Class members' personal information on its inadequately protected network.

4. As a result of Defendant's inadequate cybersecurity, the Data Breach occurred, and Plaintiffs' and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings. Plaintiffs bring this action on behalf of themselves and all Illinois and nationwide residents whose PII/PHI was exposed as a result of the Data Breach that occurred on or around January 17 to January 20, 2020 and first acknowledged by Defendant on March 16, 2020.

5. Plaintiffs seek, for themselves and the Class, injunctive relief, actual and other economic damages, consequential damages, nominal damages or statutory damages, punitive damages, and attorneys' fees, litigation expenses and costs.

VENUE AND JURISDICTION

6. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving more than 100 Class members, the amount in controversy exceeds $5 million exclusive of interest and costs, and many members of the Class are citizens of states different from Defendant.

7. This Court has personal jurisdiction over Defendant because Defendant is headquartered and has its principal place of business in San Diego, California.

8. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391 because Defendant regularly conducts business in this district, unlawful acts or omissions are alleged to have occurred in this district, and Defendant is subject to personal jurisdiction in this district.

PARTIES

9. Plaintiff, Samantha Henrichsen, and her minor son, A.R., reside in Illinois.

10. Believing Defendant would implement and maintain reasonable security procedures and practices to protect their personal information, on or about December 18, 2020, Plaintiff Henrichsen, and her minor son, A.R., provided Defendant with their confidential and highly sensitive personal and private information so they could purchase an insulin pump and related products for Plaintiff A.R.—a minor. This included information such as name and contact information, clinical data regarding A.R.'s diabetes therapy, and Plaintiffs purchase and use of Tandem's insulin products and services.

11. Following purchase of the insulin pump, Plaintiffs continued to provide PII/PHI to Tandem as part of its training and support. Tandem required Plaintiff A.R. to participate in a test period where Tandem monitored his use of its insulin pump. As part of this monitoring, Plaintiffs forwarded to Tandem A.R.'s physician reports and tests that monitored and tracked his diabetes.

12. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it collected and maintained, Plaintiffs' PII/PHI was accessed and exfiltrated, stolen or disclosed in the Data Breach.

13. Tandem Diabetes Care, Inc. is a corporation organized under the laws of the state of Delaware, with its principal place of business located at 11075 Roselle Street, San Diego, California 92121. Tandem designs, manufactures, sells and supports insulin pumps and related products, including disposable cartridges. Tandem manufactures its insulin pumps and disposable cartridges at its facility in San Diego, California.

///

///

///

///

///

FACTUAL ALLEGATIONS

PII/PHI Is a Valuable Property Right

14. PII/PHI is a valuable property right.[2] In a Federal Trade Commission ("FCC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[3]

15. The value of PII/PHI as a commodity is measurable.[4] "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[5] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market" for several years.

16. Companies recognize PII/PHI as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[6]

---

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

[3] Federal Trade Commission, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), *available at* https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

[4] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market* (April 28, 2014), *available at* http://www.medscape.com/viewarticle/824192.

[5] *See* Soma, *Corporate Privacy Trend, supra*.

[6] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

17. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

18. PHI is particularly valuable. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[7] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen social security or credit card number.[8]

19. Recognizing the high value that consumers place on their PII/PHI, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender

[7] Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market* (July 16, 2013), *available at* https://www.scmagazine.com/home/security-news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/.

[8] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014) *available at* https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

of their PII/PHI.[9] This business has created a new market for the sale and purchase of this valuable data.[10]

20. Consumers place a high value not only on their PII/PHI, but also on the *privacy* of that data. Researchers shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[11]

21. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per website.[12]

22. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

23. Theft of PII/PHI is serious. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a

---

[9] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/business/18unboxed.html.

[10] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/SB10001424052748703529004576160764037920274

[11] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1#page_scan_tab_contents.

[12] II–Horn, Hann et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* https://ideas.repec.org/p/wpa/wuwpio/0304001.html (emphasis added).

person's name.[13] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

24. 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." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[14]

25. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[15] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receive bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[16]

---

[13] *See* http:///www.gao.gov/new.items/d07737.pdf.

[14] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[15] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[16] *See* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

26. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[17] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[18] "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[19]

27. A report published by the World Privacy Form and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

[17] Pam Dixon, et al., *The Geography of Medical Identity Theft* (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf.

[18] *See* https://publicintelligence.net/fbi-health-care-cyber-intrusions/ (FBI, April 8, 2014).

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

- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.

28. A person whose PII/PHI has been compromised may not see any signs of identity theft for years. 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."

29. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[20]

30. It is within this context that Plaintiffs and thousands of Tandem diabetes customers must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Tandem's Business

31. Tandem designs, manufactures, and sells insulin pumps for which it provides ongoing support. andem also sells disposable products that are used together with its pumps and are replaced every few days, including cartridges for storing and delivering insulin, and infusion sets that connect the insulin pump to a user's body.

[20] *See* https://blog.linkedin.com/2016/05/18/protecting-our-members.

32. Tandem sells its insulin pumps and related products directly to individual customers and through third-party distributors that resell the product to insulin-dependent diabetes customers.

33. Tandem generates significant revenue from ongoing purchases of disposable insulin cartridges and other supplies by its current customer base. For this reason, Tandem has developed retention programs aimed at customers, their caregivers and healthcare providers, which includes offering training specific to its products, ongoing support by sales and clinical employees, and 24/7 technical support and customer service. As existing customers approach their insurance renewal date, Tandem's internal customer sales department contacts them to aid in the renewal.

34. In the four-year period ending December 31, 2019, Tandem shipped approximately 142,000 insulin pumps, which is representative of its global customer base.

Tandem's Collection of Customers' PII/PHI

35. Tandem admits that its business involves the storage and transmission of a substantial amount of confidential, personal, or other sensitive information, including health information and other personal information relating to its customers.

36. Tandem details the information it collects in its Privacy Policy.[21] According to its Privacy Policy, Tandem collects personal data customers voluntarily provide when interested in buying a Tandem pump. This includes customer names and contact details, insurance or other public health benefit information, and information about a customer's health and medical diagnosis and treatment. For instance, Tandem's "Health and Product Questionnaire" asks for detailed information about a prospective customer's health, including birth date, height, weight, diabetes diagnosis and medical conditions.

[21] *See* https://www.tandemdiabetes.com/privacy/privacy-policy.

37. Tandem also collects personal information from customers after they purchase an insulin pump and sign up for a t:connect account. t:connect is a cloud-based data management application that was introduced by Tandem in 2013. It provides users, their caregivers and their healthcare providers a fast, easy and visual way to display therapy management data from Tandem's pumps and supported blood glucose meters. This application empowers people with diabetes, as well as their caregivers and healthcare providers, to quickly and easily identify meaningful insights and trends, allowing them to refine therapy and lifestyle choices for better management of their diabetes.

38. According to Tandem, its insulin pumps hold the data generated over a period of up to 90 days and once a user uploads their therapy management information to t:connect, the information is retained in their t:connect account. Tandem promises that t:connect maintains the highest standards of patient data privacy and is hosted on secure servers that are compliant with the Health Insurance Portability and Accountability Act of 1996, or HIPAA.

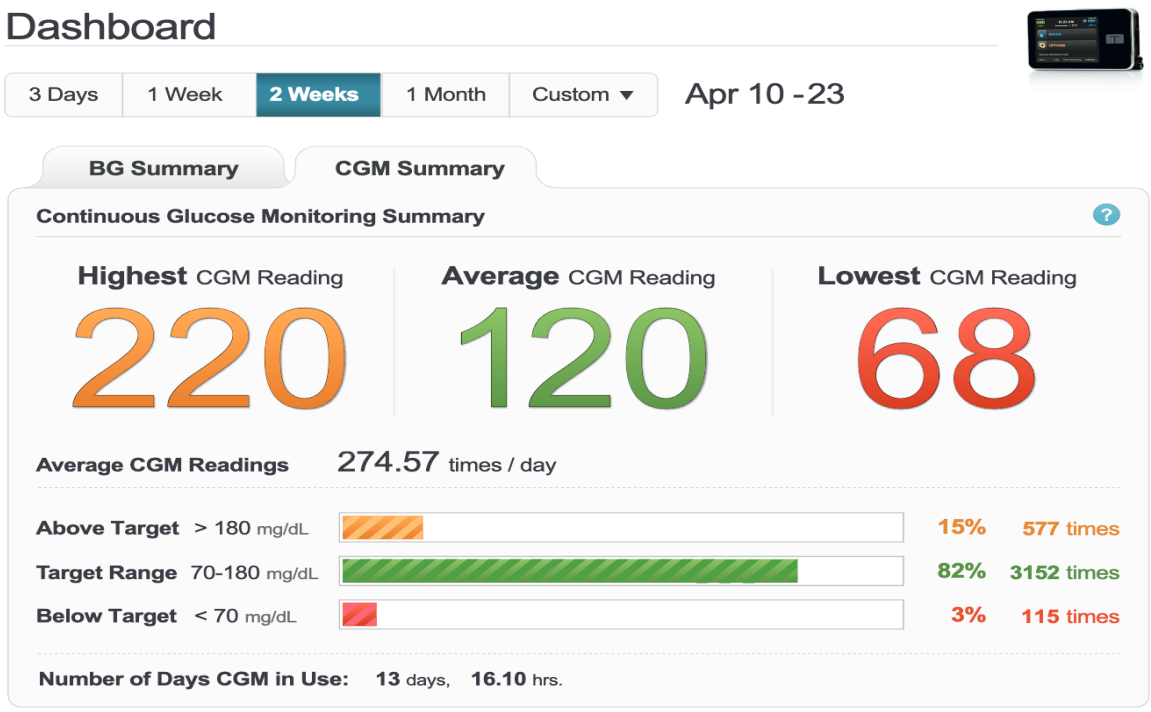
39. The data collected and transmitted via the t:connect applications includes customer names, email addresses and passwords, security questions, dates of birth, data obtained from insulin pumps, blood glucose information, and any personal data customers include in the notes field to share with their providers. This data is collected when customers create a t:connect account; when they upload pump data to the t:connect application; and when customers connect to their t:connect application.

40. The t:connect applications allow patients to track their blood sugar measurements and track goals. For instance, the t:connect web application's Dashboard gives a quick snapshot of a customer's diabetes data. The data includes:

- BG levels
- A summary of insulin usage
- BG Test Frequency
- Cartridge Change Frequency

- Infusion Set Change Frequency
- Notifications, such as whether the pump settings have been modified

41. The Dashboard looks like this:



42. Several standard reports are available to customers through Tandem's applications and contain detailed medical information. These include:

- Dashboard – Provides a general overview including highest, lowest, and average readings, and general insulin use.
- Therapy Timeline – Shows glucose readings, basal insulin delivery, and boluses over time. Continuous Glucose Monitoring ("CGM") data and suspension events are displayed, if available.
- BG Trends – Highlights time of day(s) of the week that blood glucose ("BG") tends to run high or low.
- Activity Summary – Shows the breakdown of CGM values (if applicable), BG values, insulin delivery, and bolus usage summaries.
- CGM Hourly Report – Shows hourly summary of CGM readings for one or more days and a summary of CGM readings by time of day.

- Pump Settings – Displays pump settings including Personal Profiles, Alerts, and Reminders

43. Patients can add notes to document what happened on a specific day, which can help when interpreting data. For example, a note stating that they exercised more than usual or ate a large meal at a restaurant may help explain high or low BG readings.

44. Tandem also collects credit card information, including credit card number, card expiration data, and CVC code, from customers that purchase a product or accessory directly from Tandem.

45. Tandem collects a customer's personal data by phone, email, facsimile, online application, or post that is provided by their healthcare provider(s) or representative. This information includes prescriptions and statements of medical necessity, laboratory and chart notes, and blood glucose logs.

46. Customers may also receive training from Tandem, or one of its contractors, on how to use Tandem's pump systems (including the pump, continuous glucose monitoring products, insulin cartridges, and infusion sets) and other related accessories and applications. Training may be offered in-person, through online communication systems (such as Skype or Tandem's online customer portal) or through other channels. The personal information Tandem collects from customers during training events may include a customer's name, date of birth, pump serial number, healthcare provider name, information about their current health and health history, date of training, and information about their t:connect account.

47. From time to time, Tandem may send customers an electronic survey or questionnaire about topics relating to their current health and health history, personal preferences, or personal experiences using Tandem products or services, including its pump systems and related accessories and applications.

Tandem Promises to Safeguard Customer PII/PHI

48. Tandem promises customers that it is firmly committed to their privacy and has implemented policies and practices that protect their PII/PHI.

49. Tandem claims to have implemented physical, administrative, and technical safeguards as recommended in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules to ensure customer PHI is kept safe and secure in Tandem's systems. It says 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."

50. According to Tandem, the information it collects from customers is stored in its virtual and physical databases, on its workforce's mobile electronic devices (such as cell phones, laptops, or tablets), and may be archived on physical media (such as tape).

51. Tandem promises that its servers on which it stores patient data are highly secure and are designed to comply with HIPAA, as well as applicable U.S state privacy laws (including, but not limited to, the California Consumer Privacy Act). It also assures customers that it strives to maintain and regularly update reasonable security measures, and to respond quickly and effectively if and when data security incidents do occur.

52. Despites its promises, Tandem's 10-K for fiscal year ended December 31, 2019, acknowledges that "[f]rom time to time" it has experienced various threats to its information technology systems, and that it was "currently investigating the extent of unauthorized access to data on our networks following a recent phishing attack. As a result of the ongoing investigation we may determine that substantial confidential, personal or other sensitive information was compromised, and in that case we may be subject to regulatory proceedings and substantial fines, penalties and expenses, as well as significant reputational harm, which may have a material adverse

impact on us. We are unable to predict the direct or indirect impact of any such incidents to our business."

53. Tandem acknowledges that its information technology systems, including those that support t:connect, its mobile applications, and its Tandem Device Updater, are vulnerable to damage or interruption from among other things hackers, malware, ransomware or other destructive software, and cyberattacks. It further recognizes, that should any of those risks occur, "it could adversely impact the availability, confidentiality and integrity of information assets contained in those systems."

The Data Breach

54. On March 16, 2020, Tandem reported on its website and to the California Attorney General a data breach. According to Tandem, on January 17, 2020, it discovered that an unauthorized person had gained access to an employee's email account through a phishing incident. After an investigation, the manufacturer determined that the unauthorized person had access to five employee email accounts between January 17 and January 20, 2020.

55. Tandem's notice of the data breach fails to provide any detail about what PII/PHI was accessed and by who. Tandem states only that its 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.

56. Although Tandem's notice indicates it first learned of the data breach on January 17, 2020, Tandem's 10-K for fiscal year ended December 31, 2019, says that it was "currently investigating the extent of unauthorized access to data on our networks following a recent phishing attack."

57. Tandem offers its customers nothing to assist them with any fall-out from the breach or to advise them of the potential threat they face as a result of their

sensitive PII/PHI being in the hands of criminals. Instead, Tandem "recommends that customers review billing statements from their healthcare providers and contact the provider if they are asked to pay for services not received. For those customers whose Social Security numbers were involved, the Company is offering a complimentary membership of credit monitoring and identity protection services."

58. In response to the data breach, Tandem's president and CEO stated that Tandem "take[s] the protection of our customer data very seriously, and regrettably, we did not meet the high standard we set to prevent this type of phishing attack from occurring." He promised, albeit after the breach, that Tandem is "continuing to invest in cyber security and data protection safeguards. In addition, we are implementing additional email security controls and strengthening our user authorization and authentication processes."

Tandem Knew or Should Have Known PII/PHI Are High Risk Targets

59. Tandem knew or should have known that PII, and in particular, PHI, are high risk targets for identity thieves. In 2014, the FBI informed that "[c]yber actors will likely increase cyber intrusions against healthcare systems" and warned that the "healthcare industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures[.]"[22]

60. The Identity Theft Resource Center reported that the Medical/Healthcare sector had the second largest number of breaches in 2018 and the highest rate of exposure per breach. According to the ITRC this sector suffered 363 data breaches exposing over 9 million records in 2018.[23] These included Blue Cross Blue Shield of Michigan (15K records exposed), Atrium Health (over 2M records exposed),

[22] *See* https://publicintelligence.net/fbi-health-care-cyber-intrusions/ (FBI, April 8, 2014).

[23] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, *available at* https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

UnityPoint Health (over 1M records), LifeBridge Health (over 500K), FastHealth Corporation (over 600K records), among others.

61. Tandem acknowledges that "[f]rom time to time" it has "experienced various threats to our information technology system[.]"

62. As such, Tandem was aware that PHI is at high risk of theft, and consequently should have but did not take appropriate and standard measures to protect Plaintiffs' and Class members' PII/PHI against cyber-security attacks that Tandem should have anticipated and guarded against.

CLASS DEFINITION AND ALLEGATIONS

63. Plaintiffs bring all claims as class claims under Federal Rule of Civil Procedure 23(b)(1), (b)(2), (b)(3), and (c)(4).

64. Plaintiffs bring all claims on behalf of a proposed Nationwide Class and Illinois Sub-Class, defined as follows:

> Nationwide Class: All persons in the United States whose PII/PHI was accessed by and disclosed to unauthorized persons in the Data Breach.
>
> Illinois Sub-Class: All persons in the State of Illinois whose PII/PHI was accessed by and disclosed to unauthorized persons in the Data Breach.

65. Excluded from the Class/Sub-Class are: (1) Defendant and its officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

66. **Numerosity.** While the exact number of Class/Sub-Class members is unknown, Defendant acknowledges the Data Breach, which included PII/PHI information of Defendant's customers including Plaintiffs and Class/Sub-Class members. Tandem estimates a U.S. customer base of approximately 142,000 people. Plaintiffs therefore believe that the Class/Sub-Class is so numerous that joinder of all members is impractical.

67. **Typicality.** Plaintiffs' claims are typical of the claims of the Class/Sub-Class. Plaintiffs, like all proposed members of the Class/Sub-Class, had their PII/PHI compromised in the Data Breach. Plaintiffs and Class/Sub-Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class/Sub-Class members.

68. **Commonality.** Common questions of law and fact exist as to all Class/Sub-Class members and predominate over any individual questions. Such common questions include, but are not limited to:

(a) Whether Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII/PHI it collected from Plaintiffs and Class/Sub-Class members;

(b) Whether Defendant breached its duties to protect the PII/PHI of Plaintiffs and each Class/Sub-Class member; and

(c) Whether Plaintiffs and each Class/Sub-Class member are entitled to statutory damages, actual damages, and other equitable relief.

69. **Adequacy.** Plaintiff, Samantha Henrichsen, will fairly and adequately protect the interests of the Class/Sub-Class members. Plaintiff Heinrichsen is an adequate representative of the Class/Sub-Class in that she has no interests adverse to or that conflict with the Class/Sub-Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

70. **Superiority.** A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class/Sub-Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class/Sub-Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class/Sub-Class may

be relatively small. Even if the Class/Sub-Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION

Violation of the California Confidentiality of Medical Information Act (Civil Code §§ 56, *et seq.*)

(Plaintiffs and Nationwide Class Against Defendant)

71. Plaintiffs re-allege and incorporate by reference all proceeding paragraphs as if fully set forth herein.

72. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

73. Tandem is a "contractor" within the meaning of Civil Code § 56.05(d) and/or "provider of health care" within the meaning of Civil Code § 56.06 and/or a "business organized for the purpose of maintaining medical information" and/or a "business that offers software or hardware to consumers . . . that is designed to maintain medical information" within the meaning of Civil Code § 56.06(a) and (b), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients" of Defendant, within the meaning of Civil Code § 56.05(k).

74. Plaintiff A.R. and all members of the Nationwide Class are "patients" within the meaning of Civil Code § 56.05(k) and are "endanger[ed]" within the meaning of Civil Code § 56.05(e) because Plaintiff and the Nationwide Class fear that disclosure of their medical information could subject them to harassment or abuse.

75. Plaintiffs A.R. and Nationwide Class members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network at the time of the breach.

76. Defendant, through inadequate security, allowed an unauthorized third party to gain access to Plaintiff's and each Nationwide Class members' medical information, without the prior written authorization of Plaintiff and the Nationwide Class, as required by Civil Code § 56.10 of the CMIA.

77. Defendant violated Civil Code § 56.101 of the CMIA through its failure to maintain and preserve the confidentiality of the medical information of Plaintiff A.R. and the Nationwide Class.

78. As a result of Defendant's above-described conduct, Plaintiff A.R. and the Nationwide Class have suffered damages from the unauthorized release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101.

79. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff A.R. and Nationwide Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

80. Plaintiffs, individually and for each member of the Nationwide Class, seeks nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to $3,000 per Plaintiff and each Nationwide Class member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35

SECOND CAUSE OF ACTION

Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act 815 Ill. Comp. Stat. §§ 505/1, *et seq*. ("Illinois CFA")

(Plaintiffs and Illinois Sub-Class Against Defendant)

81. Plaintiffs re-allege and incorporate by reference all proceeding paragraphs as if fully set forth herein.

82. Plaintiffs and the Illinois Sub-Class are "consumers" as that term is defined in 815 ILCS § 505/1(e). Plaintiffs and the Illinois Sub-Class and Tandem are "persons" as that term is defined in 815 ILCS § 505/1(c).

83. Tandem is engaged in "trade" or "commerce," including provision of services, as those terms are defined under 815 ILCS § 505/1(f).

84. Tandem engages in the "sale" of "merchandise" (including services) as defined by 815 ILCS § 505/1(b) and (d).

85. Tandem engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the Illinois CFA) in violation of the Illinois CFA, including but not limited to the following:

- failing to maintain sufficient security to prevent Plaintiffs' and Illinois Sub-Class members' PII/PHI from being hacked and stolen;
- misrepresenting material facts to Plaintiffs' and Illinois Sub-Class members' in connection with the sale of goods and services, by

representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs' and Illinois Sub-Class members' PII/PHI from unauthorized disclosure, release, data breaches, and theft;

- misrepresenting material facts to Plaintiffs' and the Illinois Sub-Class, in connection with sale of goods and services, by representing that Tandem did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiffs' and Illinois Sub-Class members' PII/PHI; and
- failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and Illinois Sub-Class members' PII/PHI and other personal information from further unauthorized disclosure, release, data breaches, and theft.

86. In addition, Tandem intended that Plaintiffs and the Illinois Sub-Class rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with Tandem's offering of goods and services and incorporating Plaintiffs' and Illinois Sub-Class members' PII/PHI on its servers, in violation of the Illinois CFA.

87. Tandem also engaged in unfair acts and practices by failing to maintain the privacy and security of Plaintiffs' and Illinois Sub-Class members' PII/PHI, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the HIPAA Privacy and Security Rules and similar state laws.

88. Tandem's wrongful practices occurred in the course of trade or commerce.

89. Tandem's wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Tandem that applied to Plaintiffs and all Illinois Sub-Class members and were repeated continuously before and after Tandem obtained PII/PHI from Plaintiffs and Illinois Sub-Class members. All Class members have been adversely affected by Tandem's conduct and the public was and is at risk as a result thereof.

90. Tandem also violated 815 ILCS § 505/2 by failing to immediately notify affected customers of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act ("Illinois PIPA"), 815 ILCS §§ 530/1, *et. seq.*, which provides, at Section 10:

> Notice of Breach.
>
> (a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.

91. 815 ILCS § 530/20 provides that a violation of 815 ILCS § 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

92. As a result of Tandem's wrongful conduct, Plaintiffs and Illinois Sub-Class members were injured in that they never would have allowed their PII/PHI – the value of which Plaintiffs and Illinois Sub-Class members no long have control – to be provided to Tandem if they had been told or knew that Tandem failed to maintain sufficient security to keep such data from being hacked and taken by others.

93. Tandem's unfair and/or deceptive conduct proximately caused Plaintiffs' and Illinois Sub-Class members' injuries because, had Tandem

maintained customer PII/PHI with adequate security, Plaintiffs and Illinois Sub-Class members would not have lost it.

94. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the Illinois CFA, Plaintiffs and Illinois Sub-Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity and medical theft and identity and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the Illinois CFA and PIPA, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

95. Pursuant to 815 ILCS § 505/10a(a), Plaintiffs seek actual, compensatory, and punitive damages (pursuant to 815 ILCS § 505/10a(c)), injunctive relief, and court costs and attorneys' fees as a result of Tandem's violations of the Illinois CFA.

THIRD CAUSE OF ACTION

Violations of the Illinois Uniform Deceptive Trade Practices Act 815 Ill. Comp. Stat. §§ 510/1, *et seq*. ("Illinois DTPA")

(Plaintiffs and Illinois Sub-Class Against Defendant)

96. Plaintiffs re-allege and incorporate by reference all proceeding paragraphs as if fully set forth herein.

97. Plaintiffs, the Illinois Sub-Class, and Tandem are "persons" as defined in 815 ILCS § 510/1(5).

98. The Illinois DTPA broadly prohibits deceptive trade practices. As set forth herein, Tandem failed to safeguard Plaintiffs' and Illinois Sub-Class members' PII/PHI. Accordingly, Tandem has engaged in deceptive trade practices as defined in 815 ILCS § 510/2.

99. Tandem's actions as set forth above occurred in the conduct of trade or commerce.

100. Tandem knew or should have known that its conduct violated the Illinois DTPA.

101. Tandem's conduct was material to Plaintiffs and the Illinois Sub-Class.

102. As set forth herein, Plaintiffs and the Illinois Sub-Class suffered ascertainable loss caused by Tandem's violations of the Illinois DTPA, which proximately caused injuries to Plaintiffs and the other class members.

103. Pursuant to 815 ILCS § 510/3, Plaintiffs and the Illinois Sub-Class are entitled to an award of injunctive relief to prevent Tandem's deceptive trade practices and, because Tandem's conduct was willful, an award of reasonable attorneys' fees.

FOURTH CAUSE OF ACTION

Negligence

(Plaintiffs and All Classes Against Defendant)

104. Plaintiffs re-allege and incorporate by reference all proceeding paragraphs as if fully set forth herein.

105. Defendant has (and continues to have) a duty to Plaintiffs and Class/Sub-Class members to exercise reasonable care in safeguarding and protecting their PII/PHI.

106. Defendant also had (and continues to have) a duty to use ordinary care in activities from which harm might be reasonably anticipated (such as in the storage and protection of private, non-public PII/PHI within their possession, custody and control). Such affirmative duties also are expressly imposed upon Defendant from other sources enumerated herein.

107. Defendant's duties arise from, *inter alia*, the California CMIA, the Illinois CFA, PIPA, DTPA, and the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA 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 (collectively, "HIPAA Privacy and Security Rules").

108. The above-outlined standards and duties exist for the express purpose of protecting Plaintiffs, Class/Sub-Class members and their PII/PHI.

109. Defendant violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class/Sub-Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it – including Plaintiffs' and Class/Sub-Class members' PII/PHI.

110. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class/Sub-Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class/Sub-Class members' PII/PHI for no lawful purpose.

111. Defendant, by and through its above negligent or grossly negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached its duties to Plaintiffs and Class/Sub-Class members by, among other things, failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class/Sub-Class members' PII/PHI within its possession, custody and control. Defendant, by and through its above negligent or grossly actions, inactions, omissions, and want of ordinary care, further breached its duties to Plaintiffs and Class/Sub-Class members

by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting its customers' PII/PHI.

112. But for Defendant's negligent or grossly negligent breach of the above-described duties owed to Plaintiffs and Class/Sub-Class members, their PII/PHI would not have been released, disclosed, and disseminated—without their authorization—and compromised.

113. Plaintiffs' and Class/Sub-Class members' PII/PHI was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated to unauthorized persons without their authorization as the direct and proximate result of Defendant's failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with applicable laws and safeguarding and protecting Plaintiffs' and Class/Sub-Class members' PII/PHI.

114. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach constitute negligence, gross negligence, and negligence *per se* under Illinois common law.

115. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class/Sub-Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity and medical theft, and identity and medical fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the California CMIA and the Illinois CFA, PIPA, DTPA, (v) deprivation of the value of their PII/PHI, for which there is a well-

established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

FIFTH CAUSE OF ACTION

Invasion of Privacy

(Plaintiffs and All Classes Against Defendant)

116. Plaintiffs re-allege and incorporate by reference all proceeding paragraphs as if fully set forth herein.

117. Plaintiffs and Class/Sub-Class members have a legally protected privacy interest in their PII/PHI that Defendant required them to provide and allow it to store.

118. Plaintiffs and Class/Sub-Class members reasonably expected that their PII/PHI would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

119. Defendant unlawfully invaded the privacy rights of Plaintiffs and Class/Sub-Class members by (a) failing to adequately secure their PII/PHI from disclosure to unauthorized parties for improper purposes; (b) disclosing their PII/PHI to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their PII/PHI to unauthorized parties without the informed and clear consent of Plaintiffs and Class/Sub-Class members. This invasion into the privacy interest of Plaintiffs and Class/Sub-Class members is serious and substantial.

120. In failing to adequately secure Plaintiffs' and Class/Sub-Class members' PII/PHI, Defendant acted in reckless disregard of their privacy rights. Defendant knew or should have known that its substandard data security measures are highly offensive to a reasonable person in the same position as Plaintiffs and Class/Sub-Class members.

121. Defendant violated Plaintiffs' and Class/Sub-Class members' right to privacy under the common law as well as under state and federal law.

122. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiffs' and Class/Sub-Class members' PII/PHI has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiffs and the proposed Class/Sub-Class members have suffered injury as a result of Defendant's unlawful invasions of privacy and are entitled to appropriate relief.

SIXTH CAUSE OF ACTION

Breach of Contract

(Plaintiffs and All Classes Against Defendant)

123. Plaintiffs re-allege and incorporate by reference all proceeding paragraphs as if fully set forth herein.

124. Plaintiffs and Class/Sub-Class members, upon information and belief, entered into express contracts with Defendant that included Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathered on its own, from disclosure.

125. Plaintiffs and Class/Sub-Class members performed their obligations under the contracts when they provided their PII/PHI to Defendant in relation to their purchase of its insulin pumps and related products and services.

126. Defendant breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was exposed as part of the Data Breach.

127. As a direct and proximate result of the Data Breach, Plaintiffs and Class/Sub-Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

SEVENTH CAUSE OF ACTION

Breach of Implied Contract

(Plaintiffs and All Classes Against Defendant)

128. Plaintiffs re-allege and incorporate by reference all proceeding paragraphs as if fully set forth herein.

129. Defendant provided Plaintiffs and Class/Sub-Class members with an implied contract to protect and keep their PII/PHI private.

130. Plaintiffs and Class/Sub-Class members would not have provided their PII/PHI to Defendant or its subsidiaries or contractors, but for Defendant's implied promises to safeguard and protect their information.

131. Plaintiffs and Class/Sub-Class members performed their obligations under the implied contract when they provided their PII/PHI to Defendant for its insulin pump and related products and services.

132. Defendant breached the implied contract with Plaintiffs and Class/Sub-Class members by failing to protect and keep private their PII/PHI.

133. As a direct and proximate result of Defendant's breach of its implied contract, Plaintiffs and Class/Sub-Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

EIGHTH CAUSE OF ACTION

Unjust Enrichment

(Plaintiffs and All Classes Against Defendant)

134. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

135. This claim is plead in the alternative to the above implied contract claim.

136. Plaintiffs and Class/Sub-Class members conferred a monetary benefit upon Tandem in the form of monies paid for the purchase of medical supplies and services.

137. Tandem appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class/Sub-Class members. Tandem also benefited from the receipt of Plaintiffs' and Class/Sub-Class members' PII/PHI, as this was utilized by Tandem to provide services and facilitate payment to it.

138. The monies that Plaintiffs and Class/Sub-Class members paid to Tandem were supposed to be used by Tandem, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

139. As a result of Tandem's conduct, Plaintiffs and Class/Sub-Class members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and Class/Sub-Class members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

140. Under principals of equity and good conscience, Tandem should not be permitted to retain the money belonging to Plaintiffs and Class/Sub-Class members because Tandem failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class/Sub-Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

141. Tandem should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class/Sub-Class members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

NINTH CAUSE OF ACTION

Declaratory Relief

(Plaintiffs and All Classes Against Defendant)

142. Plaintiffs re-allege and incorporate by reference all proceeding paragraphs as if fully set forth herein.

143. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's duties to safeguard and protect Plaintiffs' and Class/Sub-Class members' PII/PHI. Defendant's PII/PHI security measures were (and continue to be) woefully inadequate. Defendant disputes these contentions and contends that its security measures are appropriate.

144. Plaintiffs and Class/Sub-Class members continue to suffer damages, other injury or harm as additional identity and financial theft and fraud occurs.

145. Therefore, Plaintiffs and Class/Sub-Class members request a judicial determination of their rights and duties, and ask the Court to enter a judgment declaring, *inter alia*, (i) Defendant owed (and continues to owe) a legal duty to safeguard and protect Plaintiffs' and Class/Sub-Class members' confidential and sensitive personal information, and timely notify them about the Data Breach, (ii) Defendant breached (and continues to breach) such legal duties by failing to safeguard and protect Plaintiffs' and Class/Sub-Class members' personal information, and (iii) Defendant's breach of its legal duties directly and proximately caused the Data Breach, and the resulting damages, injury, or harm suffered by Plaintiffs and Class/Sub-Class members. A declaration from the Court ordering Defendant to stop its illegal practices is required. Plaintiffs and Class/Sub-Class members will otherwise continue to suffer harm as alleged above.

PRAYER FOR RELIEF

146. **Damages.** As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class/Sub-Class members suffered (and will continue to suffer) actual and statutory damages and other injury and harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the California CMIA

and the Illinois CFA, PIPA, DTPA, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages. Plaintiffs and Class/Sub-Class members also are entitled to equitable relief, including, without limitation, restitution. Plaintiffs' and Class/Sub-Class members' damages were foreseeable by Defendant and exceed the minimum jurisdictional limits of this Court. All conditions precedent to Plaintiffs' and Class/Sub-Class members' claims have been performed and occurred.

147. **Punitive Damages.** Plaintiffs and Class/Sub-Class members also are entitled to punitive damages from Defendant, as punishment and to deter such wrongful conduct in the future, pursuant to, *inter alia*, 815 ILCS § 505/10a and Illinois common law. All conditions precedent to Plaintiffs' and Class/Sub-Class members' claims have been performed and occurred.

148. **Injunctive Relief.** Pursuant to, *inter alia*, the Illinois CFA and DTPA, Plaintiffs and Class/Sub-Class members also are entitled to injunctive relief in multiple forms including, without limitation, (i) credit monitoring, (ii) Internet monitoring, (iii) identity theft insurance, (iv) prohibiting Defendant from continuing its above-described wrongful conduct, (v) requiring Defendant to modify its corporate culture and implement and maintain reasonable security procedures and practices to safeguard and protect the PII/PHI entrusted to it, (vi) periodic compliance audits by a third party to ensure that Defendant is properly safeguarding and protecting the PII/PHI in its possession, custody and control, and (vii) clear and effective notice to Class/Sub-Class members about the serious risks posed by the exposure of the personal information and the precise steps that must be taken to protect themselves. All conditions precedent to Plaintiffs' and Class/Sub-Class members' claims for relief have been performed and occurred.

149. **Attorneys' Fees, Litigation Expenses and Costs.** Plaintiffs and Class/Sub-Class members also are entitled to recover their attorneys' fees, litigation expenses and court costs in prosecuting this action.

WHEREFORE, Plaintiffs, on behalf of themselves and all members of the Class/Sub-Class respectfully request that (i) this action be certified as a class action, (ii) Plaintiff Henrichsen be designated representative of the Class/Sub-Class and (iii) Plaintiffs' counsel be appointed as counsel for the Class/Sub-Class. Plaintiffs, on behalf of themselves and members of the Class/Sub-Class further request that upon final trial or hearing, judgment be awarded against Defendant for:

(i) actual and punitive damages to be determined by the trier of fact;

(ii) statutory damages;

(iii) equitable relief, including restitution;

(iv) pre- and post-judgment interest at the highest legal rates applicable;

(v) appropriate injunctive relief;

(vi) attorneys' fees and litigation expenses;

(vii) costs of suit; and

(viii) such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

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

Respectfully submitted,

Dated: April 16, 2020

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
PAULA R. BROWN (254142)
JENNIFER L. MACPHERSON (202021)

By: *s/ Timothy G. Blood*
TIMOTHY G. BLOOD

501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)

tblood@bholaw.com
pbrown@bholaw.com
jmacpherson@bholaw.com

BARNOW AND ASSOCIATES, P.C.
BEN BARNOW
ERICH P. SCHORK
ANTHONY L. PARKHILL
205 W. Randolph Street, Suite 1630
Chicago, IL 60602
Tel: 312/621-2000
312/641-5504 (fax)
b.barnow@barnowlaw.com
e.schork@barnowlaw.com
aparkhill@barnowlaw.com

Attorneys for Plaintiffs