UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

SABRINA MARQUARDT, individually and on behalf of all others similarly situated, Plaintiff, v. MEDTRONIC, INC., Defendant.	Case No. _____ **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Sabrina Marquardt ("Plaintiff"), individually and on behalf of a class of similarly situated persons, brings this Class Action Complaint and alleges the following against defendant Medtronic, Inc. ("Medtronic" or "Defendant"), based upon personal knowledge with respect to Plaintiff and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Medtronic for its failure to properly secure Plaintiff's and Class Members' personally identifiable information ("PII") and personal health information ("PHI"). The PII and PHI may have included names, addresses, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as dates of birth and Social Security numbers.

2. Medtronic failed to comply with industry standards to protect information systems that contain PII. Plaintiff seeks, among other things, orders requiring Defendants to fully and accurately disclose the nature of the information that has been compromised and to adopt sufficient security practices and safeguards to prevent incidents like the disclosure (the "Data Breach") in the future.

3. On April 17, 2026, a threat actor known as ShinyHunters posted a claim on the dark web's Tor network alleging they had breached Medtronic's database. The threat actor claimed to have obtained over 9 million records containing personally identifiable information (PII), along with additional terabytes of internal corporate data.

4. On April 24, 2026, Medtronic confirmed that hackers breached Medtronic's network and exfiltrated their data.[1]

5. As a result of Medtronic's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII and PHI is now in the hands of criminals. Plaintiff and Class Members face a substantial increased risk of identity theft, both currently and for the indefinite future. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to Medtronic's failures.

6. Plaintiff seeks to remedy these harms individually and on behalf of all other similarly situated individuals whose PII was stolen in the Data Breach. Plaintiff seeks

[1] Steve Alder, Medical Device Maker Medtronic Announces Data Breach, The HIPAA Journal (Apr. 28, 2026), https://www.hipaajournal.com/medical-device-maker-medtronic-data-breach/ (last visited on Apr. 29, 2026).

remedies including compensation for time spent responding to the Data Breach and other types of harm, free credit monitoring and identity theft insurance, and injunctive relief including substantial improvements to Medtronic's data security systems.

PARTIES

7. Plaintiff Sabrina Marquardt is a resident of Catheys Valley, California, who received a Medtronic heart monitor in early 2026.

8. Defendant Medtronic, Inc. is a Minnesota corporation, with its principal office in Minneapolis, Minnesota.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists as Medtronic is a citizen of a state different from that of at least one Class Member.

10. This Court has personal jurisdiction over Medtronic because it is a resident of the State of Minnesota.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from this District. Venue is additionally proper because Medtronic transacts business and may be found in this District.

FACTUAL ALLEGATIONS

The Data Breach

12. According to Medtronic's website "Medtronic is the world leader in medical technology providing life long solutions for people with chronic disease."[2] "Medtronic has pioneered groundbreaking health tech" for the last 75 years.[3] "From the world's smallest pacemaker and advanced neurovascular care to robotic-assisted surgery, Medtronic transforms the lives of millions worldwide."[4]

13. Medtronic employs over 13,600 scientists and engineers and has over 41,000 active patents.[5] Medtronic's reported total revenue was approximately $33.5 billion dollars.[6]

14. On April 24, 2026, Medtronic stated in a press release that it had "determined that an unauthorized party accessed data in certain Medtronic corporate IT systems."[7]

---

[2] Medtronic, "U.S. patient privacy principles," https://www.medtronic.com/en-us/our-company/governance/principles-ethics/us-patient-privacy-principles.html (last accessed Apr. 29, 2026).

[3] Medtronic, "Our History," https://www.medtronic.com/en-us/our-company/history.html (last accessed Apr. 29, 2026).

[4] Medtronic, "Who We Are," https://www.medtronic.com/en-us/our-company.html (last accessed Apr. 29, 2026).

[5] Medtronic, "Who We Are," https://www.medtronic.com/en-us/our-company.html (last accessed Apr. 29, 2026).

[6] Medtronic, "Fundamentals," https://investorrelations.medtronic.com/fundamentals (last accessed Apr. 29, 2026).

[7] Medtronic, "Medtronic statement on unauthorized system access," Apr. 24, 2026, https://news.medtronic.com/Medtronic-statement-on-unauthorized-system-access (last accessed Apr. 29, 2026).

15. In the press release, Medtronic was still investigating whether patient data was impacted. "We are working to identify any personal information that may have been accessed and will provide notifications and support services as needed. We will continue to provide updates to any impacted individuals as we learn more."[8]

16. Medtronic also represented that patient privacy was an important part of their business, stating "Protecting patients and the trust placed in Medtronic is our highest priority. The privacy and security of all data with which we are entrusted is a vital part of that."[9]

17. Medtronic has not yet identified who was impacted by the data breach. Medtronic also has not explained why PII and PHI were stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the data was encrypted or otherwise protected, and whether Medtronic knows if the data has been further disseminated.

18. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, Medtronic has taken to secure the PII and PHI still in its possession. Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses the harm to Plaintiff's and Class Members' interests, and ensure that Medtronic has proper measures in place to prevent similar incidents from occurring in the future.

---

[8] *Id.*

[9] *Id.*

Medtronic's Privacy Claims

19. Medtronic acknowledges that the protection of patient information is vital to their business. "We obtain the patient information on which our business depends in accordance with applicable laws for assuring notice and choice to our customer regarding our data collection, whether our customer is the patient or a hospital, physician or other healthcare provider."[10] "Preservation of, and respect for, our customers' trust is critical to our continued success."[11]

20. Medtronic further promises to "always treat such patient information:

- Confidentially, according to applicable laws.
- Appropriately, according to the promises we make to our customers.
- Respectfully, in honor of our patients' willingness to trust us to use sensitive information to oversee the quality, safety and effectiveness of the devices that they make part of their daily lives."[12]

21. Medtronic further claims to "maintain appropriate physical, technical and administrative security standards and procedures to safeguard our patient data and systems. Our employees are educated on the importance of our privacy and security policies and must comply with them."

---

[10] Medtronic, "U.S. patient privacy principles," https://www.medtronic.com/en-us/our-company/governance/principles-ethics/us-patient-privacy-principles.html (last accessed Apr. 29, 2026).

[11] *Id.*

[12] *Id.*

The Healthcare Sector is a Primary Target for Data Breaches

22. Medtronic was on notice that companies in the healthcare industry are susceptible targets for data breaches.

23. Medtronic was also on notice that the Federal Bureau of Investigation has been concerned about data security in the healthcare industry. On April 8, 2014, the FBI's Cyber Division issued a Private Industry Notification to companies within the healthcare sector, stating that "the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs)" and pointed out that "[t]he biggest vulnerability was the perception of IT healthcare professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise." The same warning specifically noted that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or PII."[13]

[13] Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain (Apr. 8, 2014), FBI Cyber Division Private Industry Notification, https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf (last accessed Apr. 29, 2026).

24. The number of reported North American data breaches increased by over 50 percent in 2021, from 1,080 in 2020[14], to 1,638 in 2021.[15] As a recent report reflects, "[h]ealthcare has increasingly become a target of run-of-the-mill hacking attacks and the more impactful ransomware campaigns."[16]

25. At the end of 2018, the healthcare sector ranked second in the number of data breaches among measured sectors, and had the highest rate of exposure for each breach.[17] Indeed, when compromised, healthcare-related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[18] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never

---

[14] *See* Verizon 2021 Data Breach Investigations Report, at 97, https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf (last accessed Apr. 29, 2026).

[15] *See* Verizon 2022 Data Breach Investigations Report, at 83, https://www.verizon.com/business/resources/reports/dbir/2022-data-breach-investigations-report-dbir.pdf (last accessed Apr. 29, 2026).

[16] *Id.* at 62.

[17] *2018 End-of-Year Data Breach Report*, Identity Theft Resource Center, https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINALWEB-V2-2.pdf (last accessed Apr. 29, 2026).

[18] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed Apr. 29, 2026).

able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy.[19]

26. Healthcare-related breaches have persisted because criminals see electronic patient data as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the previous 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[20] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[21]

27. 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 threaten the privacy and security of patients' health and financial information, but also patient access to care.[22]

---

[19] *Id.*

[20] *2019 HIMSS Cybersecurity Survey*, https://healthsectorcouncil.org/wp-content/uploads/2019/03/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last accessed Apr. 29, 2026).

[21] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, Apr. 4, 2019, https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last accessed Apr. 29 2026).

[22] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), https://www.ama-assn.org/practice-

28. As a major vendor to healthcare providers, Medtronic knew, or should have known, the importance of safeguarding Class Members' PII and PHI entrusted to it and of the foreseeable consequences if that data was disclosed. This includes the significant costs that would be imposed on Class Members in the event of a breach. Medtronic failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Medtronic Stores Plaintiff's and Class Members' PII and PHI

29. Medtronic obtains and stores a massive amount of PII and PHI. As a condition of engaging in financial and health services, Medtronic's customers require that their own customers and patients entrust it with highly confidential PII and PHI.

30. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Medtronic assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII and PHI from disclosure.

31. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and, as current and former customers and patients of Medtronic's customers, they rely on Medtronic to keep this information confidential and securely maintained, and to make only authorized disclosures of this information.

management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Apr. 29, 2026).

PII and PHI are Valuable and Subject to Unauthorized Disclosure

32. Medtronic was aware that the PII and PHI it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

33. PII and PHI are valuable commodities to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[23] Indeed, a robust illegal market exists in which criminals openly post stolen PII and PHI on multiple underground websites, commonly referred to as the "dark web." PHI can sell for as much as $363 on the dark web, according to the Infosec Institute.[24]

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

35. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's PHI is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for

[23] Federal Trade Commission, What To Know About Identity Theft, https://consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Apr. 29, 2026).

[24] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last accessed Apr. 29, 2026).

recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[25]

36. The ramifications of Medtronic's failure to keep Class Members' PII and PHI secure are long-lasting and severe. Once PII and PHI is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for months or even years thereafter.

37. Further, criminals often trade stolen PII and PHI for years following a breach. Cybercriminals can post stolen PII and PHI on the internet, thereby making such information publicly available.

38. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. [26] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[27]

---

[25] 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 accessed Apr. 29, 2026).

[26] *See* Medical ID Theft Checklist, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last accessed Apr. 29, 2026).

[27] Experian, The Potential Damages and Consequences of Medical Identityy Theft and Healthcare Data Breaches at p. 2, https://stg1.experian.com/assets/data-breach/white-papers/consequences-medical-identity-theft.pdf (last accessed Apr. 29, 2026).

39. Here, not only PHI, but also Social Security numbers, were compromised. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt-collection calls commence months, or even years, later.[28] This time-lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

40. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

41. Changing or cancelling a stolen Social Security number is extremely difficult. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraudulent activity to obtain a new number.

---

[28] *Identity Theft and Your Social Security Number*, Social Security Administration, http://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Apr. 29, 2026).

42. Even then, a new Social Security number may not be effective. According to the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[29]

43. Medtronic knew, or should have known, the importance of safeguarding Class Members' PII and PHI entrusted to it and of the foreseeable consequences if its data-security systems were breached. This includes the significant costs that would be imposed on Class Members because of a breach. Medtronic failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

The Data Breach Exposed Plaintiff and Class Members to Identity Theft and Out-of-Pocket Losses

44. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of their rights. They are incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

45. Despite all the publicly available knowledge of the known and foreseeable consequences of disclosure of PII and PHI, Medtronic's policies and practices with respect to maintaining the security of Class Members' PII and PHI were reckless, or, at the very least, negligent.

[29] Bryan Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Apr. 29, 2026).

46. In virtually all contexts, the expenditure of time has consistently been recognized as compensable, and, for many people, it is the basis on which they are compensated. Plaintiff and Class Members should be compensated for the time they have expended because of Medtronic's misfeasance.

47. Once PII and PHI are stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[30]

48. As a result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and Class Members have and will continue to suffer financial loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their PII and PHI;

b. identity theft and fraud resulting from the theft of their PII and PHI;

c. costs associated with the detection and prevention of identity theft;

d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

[30] 2014 LexisNexis True Cost of Fraud Study, https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed Mar. 23, 2023); *see also* 2025 LexisNexis True Cost of Fraud Study, https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study (last accessed Apr. 29, 2026).

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

g. the continued imminent injury flowing from potential fraud and identify theft posed by their PII and PHI being in the possession of one or more unauthorized third parties.

Medtronic's Lax Security Violates HIPAA

49. Medtronic had a non-delegable duty to ensure that all PHI it collected and stored was secure.

50. Medtronic is bound by HIPAA (*see* 45 C.F.R. § 160.102) and, as a result, 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.

51. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable

health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

52. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

53. HIPAA requires that Medtronic implement appropriate safeguards for this information.

54. Despite these requirements, Medtronic failed to comply with its duties under HIPAA and its own Privacy Practices. In particular, Medtronic failed to:

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

b. adequately protect Plaintiff's and Class Members' PHI;

c. ensure the confidentiality and integrity of electronic PHI created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. implement technical policies and procedures for electronic information systems that maintain electronic PHI 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. implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. implement adequate 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. protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. ensure compliance with the electronic PHI security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. train all members of its workforce effectively on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their responsibilities and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b)

55. Medtronic failed to comply with its duties under HIPAA despite being aware of the risks associated with unauthorized access to Plaintiff's and Class Members' PHI.

Medtronic Violated FTC Guidelines

56. The Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, prohibited Medtronic 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' PII is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

57. The FTC has promulgated several guides for businesses that reflect the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[31]

58. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established data security guidelines for businesses.[32] The guidelines reflect that businesses should protect the PII that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

59. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to confidential data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[33]

60. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to

---

[31] Federal Trade Commission, Start With Security: A Guide for Business, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Apr. 29, 2026).

[32] Federal Trade Commission, Protecting Personal Information: A Guide for Business, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Apr. 29, 2026).

[33] FTC, *Start With Security*, *supra*.

confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data-security obligations.

61. Medtronic failed to properly implement basic data-security practices. Medtronic's failure to employ reasonable and appropriate measures to protect against unauthorized access to Class Members' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

62. Medtronic was at all times fully aware of its obligation to protect Class Members' PII and PHI because of its customers' positions as financial institutions and healthcare providers. Medtronic was also aware of the significant repercussions that would result from its failure to do so.

Plaintiff's Experience

63. In early 2026, Ms. Marquardt received an implanted Medtronic medical device.

64. Upon information and belief, Medtronic obtained Plaintiff's PII and PHI in the course of conducting its regular business operations.

65. At the time of the Data Breach, Medtronic retained Ms. Marquardt's PII and PHI.

66. Ms. Marquardt greatly values her privacy and is very careful about sharing her sensitive PII and PHI. Ms. Marquardt diligently protects her PII and PHI and takes proactive steps to ensure her PII and PHI are kept safe and secure and stores any documents containing PII and PHI in a safe and secure location. She has never knowingly

transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source.

67. Medtronic obtained and continues to maintain Ms. Marquardt's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

68. Ms. Marquardt has recently been the recipient of frequent spam calls and text messages.

69. The Data Breach has caused Ms. Marquardt to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of criminals.

70. As a result of the Data Breach, Ms. Marquardt is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

71. Ms. Marquardt has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in Medtronic's possession, are protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

72. Pursuant to Rule 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, Plaintiff seeks certification of a Class as defined below:

> All persons in the United States whose PII and/or PHI was exposed by the Data Breach that was disclosed by Medtronic on or around April 24, 2026.

73. Plaintiff further seeks certification of a California Subclass as defined below:

> All persons residing in California whose PII and/or PHI was exposed by the Data Breach that was disclosed by Medtronic on or around April 24, 2026.

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

75. Plaintiff reserves the right to modify or amend the definition of the proposed Class as additional information becomes available to Plaintiff.

76. **Numerosity:** The Class Members are so numerous that individual joinder of all Class Members is impracticable. Medtronic disclosed that over nine million records and a yet unknown or undisclosed number of its patients were affected by the Data Breach. All Class Members' names and addresses are available from Medtronic's and/or its customers' records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice-dissemination methods.

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

a. Whether and to what extent Medtronic had a duty to protect the PII and PHI of Class Members;

b. Whether Medtronic was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI;

c. Whether Medtronic had duties not to disclose the PII and PHI of Class Members to unauthorized third parties;

d. Whether Medtronic took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII and PHI;

e. Whether Medtronic failed to adequately safeguard the PII and PHI of Class Members;

f. Whether Medtronic failed to implement and maintain reasonable security policies and practices appropriate to the nature and scope of the PII and PHI compromised in the Data Breach;

g. Whether Medtronic adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

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

a. Whether Plaintiff and Class Members are entitled to restitution because of Medtronic's wrongful conduct;

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

c. Whether Plaintiff and Class Members are entitled to identity-theft protection for their respective lifetimes.

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

79. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Medtronic to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's counsel are competent and experienced in litigating class actions, including extensive experience in data-breach litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

80. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Medtronic has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Medtronic's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's

challenge of these policies hinges on Medtronic's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

81. **Superiority:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class-action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class-action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like Medtronic. Even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

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

Class Member to recover on the causes of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

84. Adequate notice can be given to Class Members directly using information maintained in Medtronic's and/or its customers' records.

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

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Class)

86. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

87. As a condition of their utilizing Medtronic's customers' services, Class Members were obligated to provide Medtronic with certain PII and PHI, including their dates of birth, Social Security numbers, personal medical information, and other PII and PHI.

88. Plaintiff and the Class Members entrusted their PII and PHI to Medtronic on the premise and with the understanding that Medtronic would safeguard their information and not disclose that information to unauthorized third parties.

89. Medtronic has full knowledge of the sensitivity of PII and PHI and the types of harm that Plaintiff and Class Members could and would suffer if PII and PHI were wrongfully disclosed.

90. Medtronic knew or should have known that the failure to exercise due care in the collection, storage, and use of Class Members' PII and PHI involved an unreasonable risk of harm to Plaintiff and Class Members.

91. Medtronic had a duty to exercise reasonable care in safeguarding, securing, and protecting Plaintiff's and Class Members' PII and PHI from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Medtronic's security protocols to ensure that Plaintiff's and Class Members' information in Medtronic's possession was adequately secured and protected, and that employees tasked with maintaining such information were adequately trained as to proper measures regarding the security of Class Members' PII and PHI.

92. Medtronic had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII and PHI.

93. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Medtronic, of failing to use reasonable measures to protect PII and

PHI. The FTC publications and orders described above also form part of the basis of Medtronic's duty in this regard.

94. Medtronic violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and PHI and failing to comply with relevant industry standards. Medtronic's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

95. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly considering the growing number of data breaches of health-care providers.

96. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Medtronic knew or should have known of the inherent risks in collecting and storing Plaintiff's and Class Members' PII and PHI, the importance of providing adequate security for that information, and that Medtronic had inadequate employee training and education and information technology security protocols in place to secure Plaintiff's and Class Members' PII and PHI.

97. Medtronic's misconduct created a foreseeable risk of harm to Plaintiff and Class Members. Medtronic's misconduct included, but was not limited to, its failure to take the steps necessary to prevent the Data Breach. Medtronic's misconduct also included its decisions not to comply with industry standards for the safekeeping and disclosure of Plaintiff's and Class Members' PII and PHI.

98. Plaintiff and Class Members had no ability to protect their PII and PHI that was in Medtronic's possession.

99. Medtronic was in a position to protect against the harm that Plaintiff and Class Members suffered as a result of the Data Breach.

100. Medtronic had and continues to have a duty to adequately disclose that Plaintiff's and Class Members' PII and PHI within Medtronic's possession might have been compromised, how it was compromised, and precisely the types of information that were compromised—and when it was compromised. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PHI by unauthorized parties.

101. Medtronic has admitted that Plaintiff's and Class Members' PII and PHI was wrongfully disclosed to unauthorized parties because of the Data Breach.

102. Medtronic, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII and PHI during the period in which that information was within Medtronic's possession or control.

103. Medtronic failed to heed industry warnings and alerts to provide adequate safeguards to protect Class Members' PII and PHI in the face of increased risk of theft.

104. Medtronic, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Class Members' PII and PHI.

105. Medtronic, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

106. But for Medtronic's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' PII and PHI would not have been compromised.

107. There is a close causal connection between Medtronic's failure to implement security measures to protect Plaintiff's and the Class Members' PII and PHI and the harm suffered or risk of imminent harm suffered by Plaintiff and Class Members. Unauthorized parties gained access to Plaintiff's and Class Members' PII and PHI as the proximate result of Medtronic's failure to exercise reasonable care in safeguarding that information by adopting, implementing, and maintaining appropriate security measures.

108. As a direct and proximate result of Medtronic's negligence, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with the effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their

PII and PHI, which remains in Medtronic's possession and is subject to further unauthorized disclosures so long as Medtronic fails to undertake appropriate and adequate measures to protect that information; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Medtronic's services that Plaintiff and Class Members received.

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

COUNT II
NEGLIGENCE PER SE
(On behalf of Plaintiff and the Class)

110. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

111. Pursuant to the FTC Act, 15 U.S.C. § 45, Medtronic had a duty to provide adequate data-security practices, including in connection with its sale of its services to Plaintiff's and Class Members' pediatric practices.

112. Pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1302d, *et seq.*, Medtronic had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' PII/PHI.

113. Medtronic breached its duties to Plaintiff and Class Members under the FTC Act and HIPAA, among other laws, by failing to provide fair, reasonable, or

adequate data security in connection with the sale and use of its services, to safeguard Plaintiff's and Class Members' PII/PHI.

114. Medtronic's failure to comply with applicable laws and regulations constitutes negligence per se.

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

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

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

118. As a direct and proximate result of Medtronic'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
VIOLATIONS OF CALIFORNIA UNFAIR COMPETITION LAW
CAL. CIV. CODE § 17200, *et seq.* ("CCPA")
(On Behalf of Plaintiff and the California Subclass)

119. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

120. Medtronic is a "person," as defined by Cal. Bus. & Prof. Code § 17201.

121. Medtronic violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

122. Medtronic's "unfair" acts and practices include:

a. Failing to implement and maintain reasonable security measures to protect Plaintiff and California Subclass members' PII and PHI from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Medtronic failed to identify foreseeable security risks and remediate identified security risks. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California Subclass, whose PII and PHI has been compromised.

b. Failing to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, HIPAA, and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5.

c. Failing to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Medtronic's inadequate security,

consumers could not have reasonably avoided the harms that Medtronic caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

123. Medtronic has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data-security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq*., the FTC Act, 15 U.S.C. § 45, HIPAA, and California common law.

124. Medtronic's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass members' PII and PHI, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common-law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California Subclass members' PII and PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common-law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California Subclass members' PII and PHI; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common-law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*.

125. Medtronic's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' PII and PHI.

126. As a direct and proximate result of Medtronic's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members were injured and lost money or property, including: the prices they paid for goods and services to

Medtronic's customers; losses from fraud and identity theft; costs for credit-monitoring and identity-protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII and PHI; and an increased, imminent risk of fraud and identity theft.

127. Medtronic acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California Subclass members' rights. Breaches within the financial and healthcare industries put Medtronic on notice that its security and privacy protections were inadequate.

128. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Medtronic's unfair, unlawful, and fraudulent business practices or use of their PII and PHI; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

129. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

130. Plaintiff and Class Members have an interest, both equitable and legal, in their PHI and PII that was conferred upon, collected by, and maintained by Medtronic and that was stolen in the Data Breach.

131. Medtronic benefitted from the conferral upon it of Plaintiff's and Class Members' PII and PHI, and by its ability to retain and use that information. Medtronic understood that it so benefitted.

132. Medtronic also understood and appreciated that Plaintiffs' and Class Members' PHI and PII was private and confidential and that its value depended upon Medtronic maintaining its privacy and confidentiality.

133. But for Medtronic's willingness and commitment to maintain its privacy and confidentiality, that PHI and PII would not have been transferred to and entrusted with Medtronic. Further, if Medtronic had disclosed that its data-security measures were inadequate, Medtronic would not have been permitted to continue in operation by regulators and the healthcare marketplace.

134. As a result of Medtronic's wrongful conduct as alleged in this Complaint (including, among other things, its utter failure to employ adequate data-security measures, its continued maintenance and use of Plaintiff's and Class Members' PHI without having adequate data-security measures, and its other conduct facilitating the theft of that PHI and PII), Medtronic has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

135. Medtronic's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compilation and use of Plaintiff's and Class Members' sensitive PHI and PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers.

136. Under the common law doctrine of unjust enrichment, it is inequitable for Medtronic to be permitted to retain the benefits it received, and is still receiving, without justification, from the use of Plaintiff's and Class Members' PHI and PII in an unfair and unconscionable manner. Medtronic's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

137. The benefit conferred upon, received, and enjoyed by Medtronic was not conferred officiously or gratuitously, and it would be inequitable and unjust for Medtronic to retain the benefit.

COUNT V
INJUNCTIVE/DECLARATORY RELIEF
(On behalf of Plaintiff and the Class)

138. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

139. Medtronic owes a duty of care to Plaintiff and Class Members requiring it to adequately secure PII and PHI.

140. Medtronic still stores Plaintiff's and Class Members' PII and PHI.

141. Since the Data Breach, Medtronic has announced no specific 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 similar incidents from occurring in the future.

142. Medtronic has not satisfied its legal duties to Plaintiff and Class Members.

143. Actual harm has arisen in the wake of the Data Breach regarding Medtronic's 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 PII and PHI, and Medtronic's failure to address the security failings that led to that exposure.

144. Plaintiff, therefore, seeks a declaration: (a) that Medtronic's existing security measures do not comply with its duties of care to provide adequate security; and (b) that to comply with its duties of care, Medtronic must implement and maintain reasonable security measures, including, but not limited to, the following:

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

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

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

d. ordering that Medtronic segment Plaintiff and Class Member data by, among other things, creating firewalls and access controls so that if one area of Medtronic's system is compromised, hackers cannot gain access to other portions of Medtronic's systems;

e. ordering that Medtronic purge, delete, and destroy in a secure manner Plaintiff and Class Member data not necessary for its provision of services;

f. ordering that Medtronic conduct regular computer-system scanning and security checks;

g. ordering that Medtronic 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

h. ordering Medtronic to meaningfully educate its current, former, and prospective customers about the threats their customers and patients face because of the loss of their PII and PHI to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

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

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

b. for equitable relief enjoining Medtronic from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII and PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

c. for equitable relief compelling Medtronic to use appropriate cyber-security methods and policies with respect to PII and PHI collection, storage, and protection, and to disclose with specificity to Class Members the types of PII and PHI compromised;

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

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

f. for prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

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

Dated: April 29, 2026

Respectfully submitted,

BRADFORD ANDRESEN NORRIE & CAMAROTTO

/s/ Nicole S. Frank

Nicole S. Frank (#0388822)
3600 American Boulevard West, Ste. 670
Bloomington, MN 55431
(612) 474-1811
nfrank@banclaw.com

BAILEY GLASSER LLP
Bart D. Cohen (*pro hac vice* forthcoming)
Panida Anderson (*pro hac vice* forthcoming)
1055 Thomas Jefferson Street NW
Suite 540
Washington, DC 20007
(202) 463-2101
bcohen@baileyglasser.com
panderson@baileyglasser.com

Attorneys for Plaintiff and the Proposed Class

ClassAction.org
