IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MICHIGAN

TOM MESMER, on behalf of himself and all others similarly situated,

Plaintiff,

v.

STRYKER CORPORATION,

Defendant.

CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiff Tom Mesmer, on behalf of himself and all others similarly situated, brings this Class Action Complaint (the "Action") against Stryker Corporation ("Stryker" or "Defendant"), and alleges upon personal knowledge as to himself and his own actions, and upon information and belief as to all other matters, as follows:

I. NATURE OF THE ACTION

1. Plaintiff brings this Class Action Complaint against Stryker for its failure to secure and safeguard personally identifiable health information ("PHI"), other personally identifiable information ("PII"), and likely other sensitive information that was entrusted to Stryker (collectively "Private Information").

2. In March 2026, Stryker experienced a cyberattack of its computer network. This cyberattack likely resulted in the breach and/or compromise of certain files containing the sensitive personal data of Plaintiff and potentially millions of other individuals, including but not necessarily limited to names, dates of birth, addresses, Social Security numbers, employment information, and

PHI (the "Data Breach").

3. Stryker, a multinational Fortune 500 company, is one of the largest manufacturers of medical devices for surgery and neurotechnology-based treatments and diagnostics in the world. Stryker, as a substantial business, had the resources available to take seriously the obligation to protect Private Information. However, Stryker failed to invest the resources necessary to protect the Private Information of Plaintiff and Class members.

4. The actions of Stryker related to this Data Breach are unconscionable. Upon information and belief, Stryker failed to implement practices and systems to mitigate against the risks posed by Stryker's negligent (if not reckless) IT practices. As a result of these failures, Plaintiff and Class members face a litany of harms that accompany data breaches of this magnitude and severity.

5. As such, Plaintiff, on behalf of himself and all others similarly situated, brings this Action for restitution, actual damages, nominal damages, statutory damages, injunctive relief, disgorgement of profits, and all other relief that this Court deems just and proper.

II. JURISDICTION AND VENUE

6. This Court has jurisdiction over the subject matter of this Action pursuant to 28 U.S.C. § 1332(d), as provided by the Class Action Fairness Act, because: this is a civil action filed under Rule 23 of the Federal Rules of Civil Procedure; the amount in controversy exceeds $5,000,000, exclusive of interest and costs; and members of the Class are citizens of a state different from Defendant, including Tennessee.

7. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is located at 2825 Airview Boulevard, Kalamazoo, Michigan, and because a substantial part of Defendant's conduct giving rise to this Action took place in the state of

Michigan.

8. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendant is a resident in this District.

III. PARTIES

9. Plaintiff Tom Mesmer is currently a resident of the state of Tennessee and was, at other times relevant to this action, a resident of the state of Florida. Plaintiff is a former employee of Defendant; he worked for Defendant as a customer service representative in Tampa from November 2017 to October 2023. Plaintiff provided his Private Information to Defendant prior to the Data Breach as a condition of, and in exchange for, employment. Upon information and belief Plaintiff's Private Information was accessed and exfiltrated by cybercriminals in the Data Breach.

10. At all times material hereto, Stryker is and was a Michigan-based manufacturer of medical devices, authorized to transact and regularly transacting business in the state of Michigan, with its principal place of business in the state of Michigan.

IV. FACTUAL ALLEGATIONS

A. Defendant's Business and Collection of Private Information

11. Stryker is a manufacturer of surgical and neurotechnological medical devices for patients throughout the United States and employs tens of thousands of individuals in the United States. Stryker's medical devices are used by hundreds of millions of patients throughout the world, including in the United States.

12. Plaintiff and the rest of the Class members were either employed by or received products or services, directly or indirectly, from Stryker, and, in doing so, entrusted Stryker with their extremely sensitive and highly valuable Private Information, which Stryker acquired from Plaintiff and the other Class members in the course of employing or providing services to them.

13. In turning over their Private Information, Plaintiff and Class members reasonably expected that Stryker would safeguard their highly sensitive and valuable information and would make only authorized disclosures of this Private Information.

14. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class members' Private Information, Stryker assumed legal and equitable duties and knew or should have known that it was responsible for ensuring the safety and security of Plaintiff's and Class members' Private Information and for protecting such Private Information from unauthorized disclosure and exfiltration.

B. The Data Breach

15. In March 2026, Stryker experienced a cyberattack of its computer network. This cyberattack, according to numerous public reports, resulted in the breach and/or compromise of at least 50 terabytes of information, which, on information and belief, contains the sensitive personal data of Plaintiff and potentially millions of other individuals, including but not necessarily limited to name, dates of birth, addresses, Social Security numbers, employment information, and PHI.

16. Not only do Plaintiff and Class members have to contend with the harms caused by the Data Breach, but Stryker's response to the Data Breach has been woefully insufficient. To date, Defendant has yet to provide any notice to the individuals impacted.

17. On information and belief, the Private Information compromised in the Stryker files accessed by the threat actors was not encrypted. In any event, the threat actors were able to access the Private Information listed above.

18. The access and/or acquisition of the Private Information from Stryker's systems demonstrates that this cyberattack was targeted due to Stryker's status as a business that houses sensitive Private Information. Armed with this Private Information, data thieves (as well as

downstream purchasers of the stolen Private Information) can commit a variety of crimes, including as follows: opening new financial accounts in Class members' names, taking out loans in Class members' names, using Class members' information to obtain government benefits, filing fraudulent tax returns using Class members' identification information, obtaining driver's licenses in Class members' names but with different photographs, giving false information to police during any arrests, and receiving medical benefits in Class member's names.

19. Due to Stryker's flawed security measures and Stryker's incompetent response to the Data Breach, Plaintiff and Class members now face a present, substantial, and imminent risk of fraud and identity theft and must deal with that threat forever.

20. Despite widespread knowledge of the dangers of identity theft and fraud associated with cyberattacks and unauthorized disclosure of Private Information, and despite Stryker's large operating budget, Stryker maintained unreasonably deficient protections prior to the Data Breach, including but not limited to a lack of security measures for storing and handling Private Information, as well as inadequate employee training regarding how to access, oversee the protection of, and handle and safeguard this sensitive set of information.

21. Stryker also failed to adequately adopt and train its employees on even the most basic of information security protocols, including storing, locking, encrypting, and limiting access to Plaintiff's and Class members' highly sensitive Private Information; implementing guidelines for accessing, maintaining, and communicating sensitive Private Information; and protecting sensitive Private Information by implementing protocols on how to utilize, store, and handle such information.

22. Stryker's failures caused the unpermitted disclosure of Plaintiff's and Class members' Private Information to unauthorized third-party cybercriminals, and have put Plaintiff

and Class members at serious, immediate, and continuous risk of identity theft and fraud.

23. The Data Breach that exposed Plaintiff's and Class members' Private Information was caused by Stryker's violation of its obligations to abide by best practices and industry standards concerning its information security practices and processes.

24. Stryker, despite being a technologically advanced organization, failed to comply with basic security standards or to implement security measures that could have prevented or mitigated the Data Breach.

25. Stryker failed to ensure that all personnel with access to Plaintiff's and Class members' Private Information were properly trained in retrieving, handling, using, and distributing sensitive information. Stryker's personnel were also not properly trained to apply relevant updates and software patches.

C. The Data Breach Was Foreseeable

26. Stryker has weighty obligations created by industry standards, common law, and its own promises and representations to keep Private Information confidential and to protect it from unauthorized access and disclosure.

27. Plaintiff and Class members provided their Private Information to Stryker with the reasonable expectation and mutual understanding that Stryker would comply with its obligations to keep such information confidential and secure from unauthorized access.

28. Stryker's data security obligations were particularly acute given the substantial increase in hacks, malware threats, ransomware attacks, and/or other data breaches in various industries, including the industry in which Stryker operates, preceding the date of the Data Breach.

29. Stryker was aware of the risk of data breaches because such breaches have dominated the headlines in recent years.

30. Private information, like the Private Information targeted by the hackers in this Action, is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners. Private Information can be used to distinguish, identify, or trace an individual's identity. This can be accomplished alone or in combination with other personal or identifying information that is connected or linked to an individual, such as the information compromised in the Data Breach.

31. Given the nature of the Data Breach, it is foreseeable that the compromised Private Information can now be used by hackers and cybercriminals in a variety of different and harmful ways.

32. Cybercriminals who possess Plaintiff's and Class members' Private Information can (either in isolation or in tandem with other information) obtain Plaintiff's and Class members' tax returns or open fraudulent credit card or other types of accounts in Plaintiff's and Class members' names.

33. The increase in such attacks, and attendant risk of future attacks, was widely known.

34. As such, this Data Breach was foreseeable. Defendant was cognizant of the huge risk of data breaches because of how common and high-profile data breaches have become with respect to businesses that have custody of personally identifiable information, such as Stryker.

D. Defendant Failed to Follow FTC Guidelines and Industry Standards

35. Experts studying cybersecurity routinely identify individual-facing businesses as being particularly vulnerable to cyberattacks because of the value of the data which they collect and maintain. The reason this data is so valuable is because it contains sensitive details such as the Private Information, which can be sold and weaponized for purposes of committing various

identity theft-related crimes. It is well-known that, because of the value of this data and Private Information, businesses that collect, store, maintain, and otherwise utilize or profit from Private Information must take necessary cybersecurity safeguards to ensure that the data they possess is adequately protected.

36. Government agencies also highlight the importance of cybersecurity practices. For example, the Federal Trade Commission ("FTC") has promulgated numerous guides for businesses, which highlight the importance of implementing reasonable data security practices.

37. According to the FTC, the need for data security should be factored into all business decision-making.

38. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.

39. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand network vulnerabilities; and implement policies to correct any security problems.

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

41. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on their network; and verify that third-party service providers have

implemented reasonable security measures.

42. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, in some cases treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"). Orders resulting from these actions further explicate and clarify the measures businesses must take to meet their data security obligations.

43. Defendant failed to properly implement some or all of these (and other) basic data security practices.

44. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

45. Defendant at all times was fully aware of its obligations to protect Private Information. Defendant was also keenly aware of the significant repercussions that would result from the failure to do so.

46. Experts studying cybersecurity routinely identify individual-facing businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

47. Several best practices have been identified that, at a minimum, should be implemented by businesses such as Stryker that maintain personally identifiable information; these include but are not limited to the following: educating all employees about cybersecurity; requiring strong passwords; maintaining multi-layer security, including firewalls, anti-virus programs, and anti-malware software; utilizing encryption; making data unreadable without a key; implementing

multi-factor authentication; backing up data; and limiting which particular employees can access sensitive data.

48. Other best cybersecurity practices that are standard in the industry include installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; and training staff regarding critical points.

49. These foregoing frameworks are existing and applicable industry standards. Stryker failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

E. Defendant's Breaches of Its Obligations

50. Defendant breached its obligations to Plaintiff and Class members and was otherwise negligent and/or reckless because Defendant failed to properly maintain, oversee, and safeguard its computer systems, network, and data. In addition to its obligations under federal and state law, Defendant owed a duty to Plaintiff and Class members to exercise reasonable care when obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, or misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class members to provide reasonable security, including complying with industry standards and requirements, providing training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Plaintiff and Class members.

51. Defendant's wrongful conduct includes, but is not limited to, the following acts and/or omissions:

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

b. Failing to adequately protect Plaintiff's and Class members' Private Information;

c. Failing to implement updates and patches in a timely manner;

d. Failing to properly monitor third-party data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

e. Failing to ensure that all employees and third parties apply all available and necessary security updates;

f. Failing to ensure that all employees and third parties install the latest software patches, update their firewalls, check user account privileges, and ensure proper security practices;

g. Failing to ensure that all employees and third parties practice the principle of least-privilege and maintain credential hygiene;

h. Failing to avoid the use of domain-wide, admin-level service accounts;

i. Failing to adequately oversee employees and third-party vendors;

j. Failing to ensure that all employees and third parties employ or enforce the use of strong, randomized, just-in-time local administrator passwords; and

k. Failing to properly train and supervise employees and third parties in the proper handling of inbound emails.

52. As the result of allowing its computer systems to fall into dire need of security upgrading and its inadequate procedures for handling cybersecurity threats, Stryker negligently and wrongfully failed to safeguard Plaintiff's and Class members' Private Information.

53. Accordingly, as further detailed herein, Plaintiff and Class members now face a

substantial, increased, and immediate risk of fraud, identity theft, and the disclosure of their most sensitive and deeply personal information.

F. Data Breaches Are Harmful and Disruptive

54. The United States Government Accountability Office ("GAO") released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

55. That is because all victims of a data breach may be exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal Private Information is to monetize it because there is (unfortunately) a market for Private Information, like the Private Information compromised by the Data Breach.

56. Cybercriminals do this by selling the spoils of their cyberattacks on the illegal market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the greater number of accurate individual pieces of data an identity thief obtains regarding a person, the easier it is for that thief to take on the victim's identity, or otherwise to harass or track the victim.

57. For example, armed with only a name and a date of birth – just two of the many pieces of Private Information compromised in the Data Breach – a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information regarding a victim's identity, such as a person's login credentials. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls, deceptive text messages, and phishing emails.

58. Because of the threat of these harms, the FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach such as the Data Breach at issue here, including contacting one of the credit bureaus to place a fraud alert (and potentially obtaining an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, purchasing credit monitoring, and correcting their credit reports.

59. Theft of Private Information is gravely serious. Private Information is an extremely valuable property right.

60. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates that Private Information has considerable market value.

61. According to the GAO:

> [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.

See GAO Report, at p. 29.

62. Private information, such as the Private Information compromised in the Data Breach, is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. The private information of consumers remains of high value to criminals, as evidenced by the prices paid through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, certain sets of private information can be sold at a price from $40 to $200. Social

Security numbers and government-issued ID numbers, both of which were compromised in this Data Breach, are particularly valuable. Clearly, all this data has real value – which is why it is often targeted and stolen in the first place.

63. Because the Private Information compromised in the Data Breach has been dumped onto the dark web, Plaintiff and Class members are at a substantial imminent risk of injury, including an increased risk of fraud and identity theft for many years into the future.

64. Thus, Plaintiff and Class members must vigilantly monitor their financial accounts and other indicators of identity theft (*e.g.*, the mail, email, etc.) for many years to come.

G. Harm to Plaintiff and the Class

65. Plaintiff and Class members suffered actual injury from having their Private Information compromised as a result of the Data Breach, including, but not limited to, as follows: (a) misuse of their compromised Private Information; (b) damage to and diminution in the value of their Private Information, a form of property that Defendant obtained from Plaintiff and Class members; (c) violation of their privacy, including the compromise of highly sensitive Private Information; (d) present, imminent, and impending injury arising from the increased risk of identity theft and fraud; and (e) actual and potential out-of-pocket losses, including the loss of time and the loss of money.

V. CLASS ALLEGATIONS

66. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b) and 23(c) of the Federal Rules of Civil Procedure. The "Class" that Plaintiff seeks to represent is defined as follows:

> **Class Definition.** All persons whose Private Information was maintained by Stryker and was compromised in the Data Breach.

67. Excluded from the Class are Defendant and Defendant's subsidiaries, affiliates,

officers, and directors, and any entity in which Defendant has a controlling interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

68. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

69. **Numerosity**. The Data Breach compromised Private Information of potentially million individuals. Therefore, the members of the Class are so numerous that joinder of all members is impracticable.

70. **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 Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class members' Private Information;

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

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Plaintiff and Class members to safeguard their Private Information;

f. Whether Defendant breached its duties to Plaintiff and Class members to safeguard their Private Information;

g. Whether computer hackers / cybercriminals obtained Plaintiff's and Class members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's acts, inactions, and practices complained of herein amount to a breach of contract, and/or common law negligence, and whether Defendant has been unjustly enriched;

k. Whether Defendant failed to provide notice of the Data Breach in a timely and proper manner; and

l. Whether Plaintiff and Class members are entitled to compensatory damages, exemplary damages, punitive damages, civil penalties, equitable relief, and/or injunctive relief.

71. **Typicality**. Plaintiff's claims are typical of those of other Class members because Plaintiff's Private Information, like that of every other Class member, was compromised by the Data Breach. Further, Plaintiff, like all Class members, was injured by Defendant's uniform conduct. 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. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

72. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Class, and has no disabling or disqualifying conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights that Plaintiff suffered are typical of the other Class members, and Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class. Plaintiff has a genuine personal interest, not a mere technical interest, in the outcome of this Action. Plaintiff has retained counsel experienced in complex class action litigation, including, but not limited to, data privacy class action litigation, and Plaintiff intends to prosecute this Action vigorously. Therefore, Plaintiff can and will fairly and adequately protect and represent the interests of the Class.

73. **Superiority of Class Action**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class's common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in individual actions that are based upon an identical set of facts. Without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

74. The litigation of the claims brought herein is manageable. Defendant'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 prosecuting this lawsuit as a class action. This proposed class action does not present any unique management difficulties.

75. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

76. **Predominance**. The issues in this Action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Defendant has engaged in a common course of conduct toward Plaintiff and Class members. The common issues arising from Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these issues in a single action has important and desirable advantages of judicial economy.

COUNT I

NEGLIGENCE

77. Plaintiff repeats and realleges all preceding paragraphs as if fully set forth herein.

78. Plaintiff and Class members provided their Private Information to Stryker as a condition of obtaining Defendant's products or services or securing employment.

79. Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in securing, safeguarding, storing, and protecting the Private Information of Plaintiff and Class members – which Defendant collected from Plaintiff and Class members as a condition of providing its services – from being compromised, lost, stolen, accessed, or misused by unauthorized parties.

80. This duty included obligations to take reasonable steps to prevent disclosure of the Private Information, and to safeguard the information from theft. Stryker's duties included the responsibility to design, implement, and monitor its data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

81. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, its policies and procedures, and the personnel responsible for them adequately protected the Private Information.

82. Defendant owed a duty of care to safeguard the Private Information due to the foreseeable risk of data breaches and the severe consequences that would result from its failure to safeguard Private Information.

83. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and those individuals who entrusted

Defendant with their Private Information, which duty is recognized by laws and regulations, including but not limited to the FTCA and common law.

84. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the FTCA, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

85. Defendant's duty to use reasonable care in protecting Private Information arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect Private Information that it acquires, maintains, or stores.

86. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class members could and would suffer if their Private Information were wrongfully disclosed.

87. Defendant had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' willingness to entrust Stryker with Plaintiff's and Class members' Private Information as a condition of receiving services was predicated on the understanding that Stryker would take adequate security precautions to protect that Private Information.

88. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

89. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class members' Private Information, as alleged and discussed above.

90. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' Private Information would result in injury to Plaintiff and Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches against companies that have custody of PII and PHI.

91. It was therefore foreseeable that the failure to adequately safeguard Class members' Private Information would result in one or more types of injuries to Class members.

92. The imposition of a duty of care on Defendant to safeguard the Private Information it maintained, transferred, stored, or otherwise used is appropriate because any (minimal to non-existent) social utility of Defendant's conduct in failing to protect the Private Information is outweighed by the injuries suffered by Plaintiff and Class members as a result of the Data Breach.

93. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members are at a current and ongoing imminent risk of identity theft, and Plaintiff and Class members sustained compensatory damages, including the following: (i) invasion of privacy; (ii) financial out-of-pocket costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the material risk and imminent threat of identity theft; (iv) financial out-of-pocket costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) diminution of value of their Private Information; (viii) future costs of identity theft monitoring and/or credit monitoring; (ix) anxiety, annoyance, and nuisance, and (x) the continued risk to Private Information, which remains in Defendant's and the threat actors' respective control, and which is subject to further breaches, including for so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' Private Information.

94. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

COUNT II

BREACH OF IMPLIED CONTRACT

95. Plaintiff repeats and realleges all preceding paragraphs as if fully set forth herein.

96. In connection with obtaining services from Defendant, Plaintiff and Class members entrusted Defendant with their Private Information.

97. Defendant had an implied contract with Plaintiff and Class members that it would protect the Private Information it collected from them.

98. Plaintiff and Class members were required to deliver their Private Information to Defendant as part of the process of receiving products or services or employment. In doing so, they were of the belief that this information would be safely guarded.

99. Defendant accepted possession of Plaintiff's and Class members' Private Information for the purpose of providing services to them.

100. Through Defendant's individual provision of services, it knew or should have known that it must protect Plaintiff's and Class members' confidential Private Information in accordance with Defendant's stated policies and industry best practices.

101. Pursuant to these implied contracts, Defendant agreed to certain implied promises to Plaintiff and Class members, including but not limited to the following: (1) taking steps to ensure that anyone who is granted access to Private Information also protects the confidentiality of that data; (2) taking steps to ensure that the Private Information placed in control of Defendant's employees is restricted and limited only to achieve authorized business purposes; (3) restricting Private Information access only to employees and/or agents who are qualified and trained; (4)

designing and implementing appropriate retention policies to protect Private Information; (5) applying or requiring proper encryption and/or the separation of different data sets containing Private Information; (6) implementing multifactor authentication for access to Private Information; and (7) taking other steps to protect against foreseeable breaches.

102. By entering into such implied contract, Plaintiff and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

103. Defendant violated these implied contracts and these implied promises by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class members' Private Information.

104. Plaintiff's and Class members' Private Information would not have been entrusted to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

105. Plaintiff and Class members fully and adequately performed their obligations under their implied contracts with Defendant.

106. Plaintiff and Class members have been damaged by Defendant's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein. Plaintiff and Class members seek damages, including restitution, actual damages, nominal damages, and any other awardable form of damages, in an amount to be proven at trial.

COUNT III

UNJUST ENRICHMENT

107. Plaintiff repeats and realleges all preceding paragraphs as if fully set forth herein.

108. This count is asserted in the alternative to breach of implied contract (Count II).

109. Plaintiff and Class members conferred a benefit on Defendant, whereby their Private Information was provided to Defendant in the course of its provision of products or services or employment to Plaintiff and Class members.

110. Defendant, prior to and at the time Plaintiff and Class members entrusted it with Private Information, caused Plaintiff and Class members to reasonably believe that it would keep that Private Information secure.

111. The monies Defendant was paid in its ordinary course of business included a premium for Defendant's cybersecurity obligations that were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection for Plaintiff's and Class members' Private Information.

112. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures in order to secure Plaintiff's and Class members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

113. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

114. Defendant failed to secure Plaintiff's and Class members' Private Information and, therefore, did not provide full compensation to Plaintiff and Class members for the benefit Plaintiff and Class members provided.

115. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

116. Defendant failed to disclose facts pertaining to its substandard information systems, or defects and vulnerabilities therein, before Plaintiff and Class members made their decisions to provide Defendant with their Private Information.

117. Plaintiff and Class members have no adequate remedy at law.

118. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will suffer injury, including but not limited to the following: (a) actual identity theft; (b) the loss of the opportunity to control how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity 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 identity theft; (f) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures, including for so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class

members.

119. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm.

120. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that Defendant unjustly received from them. This can be accomplished by establishing a constructive trust from which Plaintiff and Class members may seek restitution or compensation.

COUNT IV

DECLARATORY JUDGMENT

121. Plaintiff repeats and realleges all preceding paragraphs as if fully set forth herein.

122. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights, statuses, and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of federal and state law as described in this Complaint.

123. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class members' Private Information and whether Stryker is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their Private Information. Plaintiff alleges that Stryker's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his Private Information and remains at imminent risk that further compromises of their Private Information will occur in the future.

124. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Stryker owes a legal duty to secure Private Information and to timely notify impacted individuals of a data breach under the common law and state statutes; and

b. Stryker continues to breach this legal duty by failing to employ reasonable measures to secure Private Information in its possession.

125. This Court also should issue corresponding prospective injunctive relief requiring Stryker to employ adequate security protocols consistent with law and industry standards to protect Private Information in Stryker's data network.

126. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Stryker. The risk of another such breach is real, immediate, and substantial. If another breach at Stryker occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and he will be forced to bring multiple lawsuits to rectify the same conduct.

127. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Stryker if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damages. On the other hand, the cost to Stryker of complying with an injunction by employing reasonable protective data security measures is relatively minimal, and Stryker has a pre-existing legal obligation to employ such measures.

128. Issuance of the requested injunction is in the public interest. Such an injunction would benefit the public by preventing another data breach at Stryker, thus eliminating the additional injuries that would result to Plaintiff and Class members whose confidential information

would be further compromised.

VI. PRAYER FOR RELIEF

129. WHEREFORE, Plaintiff, on his own behalf and on behalf of all others similarly situated, pray for relief as follows:

A. For an Order certifying this case as a class action and appointing Plaintiff and his counsel to represent the Class;

B. For an award of actual damages, exemplary damages, punitive damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

C. For injunctive and other equitable relief to ensure the protection of the sensitive information of Plaintiff and the Class, which remains in Defendant's possession;

D. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

E. Pre- and post-judgment interest on any amounts awarded; and

F. Such other and further relief as the Court may deem just and proper.

VII. JURY TRIAL DEMAND

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

DATED: March 13, 2026

Respectfully submitted,

/s/ Lisa M. Esser

Lisa M. Esser (P70628)
SOMMERS SCHWARTZ P.C.
One Towne Square, 17th Floor
Southfield, Michigan 48076
Telephone: (248) 746-4015
LEsser@sommerspc.com

Israel David (*pro hac vice* forthcoming)
Adam M. Harris (*pro hac vice* forthcoming)
ISRAEL DAVID LLC
60 Broad Street, Suite 2900
New York, New York 10004
Telephone: (212) 350-8850
israel.david@davidllc.com
adam.harris@davidllc.com

Mark A. Cianci (*pro hac vice* forthcoming)
ISRAEL DAVID LLC
399 Boylston Street, Floor 6, Suite 23
Boston, Massachusetts 02116
Telephone: (617) 295-7771
mark.cianci@davidllc.com

Attorneys for Plaintiff and the Proposed Class

ClassAction.org
