UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

LIAM MURRAY, on behalf of himself and all others similarly situated, Plaintiff, vs. ONETOUCHPOINT, INC., Defendant.	Case No.: 23-cv-301 CLASS ACTION COMPLAINT DEMAND FOR JURY TRIAL

Plaintiff Liam Murray ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against OneTouchPoint, Inc., (hereinafter "Defendant" or "OTP"), and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII") that the Defendant collected, stored, and maintained on behalf of Plaintiff and Class Members.[1] This information included, but is not limited to, names, addresses, Social Security numbers, financial account information, and Protected Health Information ("PHI"). Defendant failed to comply with industry standards to protect information systems containing that PII, and failed to provide timely, accurate, and adequate notice to Plaintiff

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number, or cellular phone location and usage data).

and Class Members that their PII had been accessed by an unauthorized third party and even precisely what types of information was unencrypted and accessed by unauthorized third parties.

2. Defendant is a corporation engaged in marketing execution, digital marketing, fulfillment, and related services provided for client companies within the United States including health insurance carriers, medical providers and financial service companies. Defendant received the information provided by individuals to their client companies for business purposes.

3. Defendant is a HIPAA covered business associate that provides services to and on behalf of various health care plans and providers or "Covered Entities" under 45 C.F.R. § 160.103. In the regular course of business, Defendant receives, collects, stores, and/or transmits Protected Health Information (PHI)[2].

4. On April 28, 2022, Defendant discovered the external system breach, or "hacking", when it found files on its system were tampered with and encrypted. An investigation revealed the breach occurred on April 27th, 2022, when its servers were compromised, and sensitive data was accessed by an unauthorized third party.[3]

5. Defendant's client companies were not notified of the breach until June 3, 2022.[4] Despite learning of the breach in April, Defendant did not begin notifying Plaintiff and Class Members until on or about July 27, 2022. Indeed, the Office of Civil Rights for the Department of Health and Human Services was not notified until July 27, 2022.[5]

---

[2] Protected Health Information means individually identifiable information including demographic information used by a HIPAA covered entity or business associate in relation to healthcare services or payment. 45 C.F.R. § 160.103.

[3] OneTouchPoint, *Notice of Data Security Event,* https://1touchpoint.com/notice-of-data-event (last visited Dec.21, 2022).

[4] *OneTouchPoint Ransomware Victim Count Increases to 2.65 Million,* HIPAAJOURNAL, (Sept. 1, 2022), https://www.hipaajournal.com/onetouchpoint-ransomware-victim-count-increases-to-2-65-million/ (last visited Dec.21, 2022).

[5] Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Dec. 21, 2022).

6. Defendant, as a HIPAA covered business associate and being in the business of providing online services to its customers, certainly was aware of its obligations to provide a speedy and comprehensive response to the Data breach including notifying those affected.

7. As a result of the Data breach, Plaintiff and over two million Class Members[6] suffered ascertainable losses in the form of losing the benefit of their bargaining, incurring out of pocket expenses, and the value of their time reasonably spent to remedy or mitigate the effects of the attack and the substantial and ongoing risk of identity theft.

8. As a condition of providing services related to healthcare providers and health insurance carriers, Defendant requires that its customers entrust it with PII. Plaintiff and Class Members provided their PII to Defendant, either directly or indirectly through Defendant's customers. Plaintiff and Class Members did so in confidence having the legitimate expectation that Defendant would respect their privacy and act appropriately.

9. In its *Notice of Data Security Event*, Defendant stated that although they were initially "unable to determine what specific files the unauthorized actor viewed within the OTP network", they later determined that "scope of information potentially involved includes an individual's name, member ID, and information that may have been provided during a health assessment."[7] According to the HIPAA Journal, "[c]ustomers have reported the breach involving names, subscriber ID numbers, diagnoses, medications, addresses, dates of birth, sexes, physician demographics information, family histories, social histories, allergies, vitals, immunizations, and other information."[8]

---

[6] *OneTouchPoint Ransomware Victim Count Increases to 2.65 Million,* HIPAAJOURNAL (Sept. 1, 2022).
[7] *Notice of Data Security Event,* https://1touchpoint.com/notice-of-data-event (last visited Dec.21, 2022).

[8] *OneTouchPoint Ransomware Victim Count Increases to 2.65 Million,* HIPAAJOURNAL (Sept. 1, 2022).

10. By obtaining, collecting, using, and deriving a benefit from the PII provided by Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting this information from unauthorized disclosure.

11. Plaintiff and Class Members face a lifetime risk of identity theft. This risk is heightened here by the sensitivity of the data accessed and/or acquired by third party bad actors.

12. The PII of Plaintiff and Class Members was subject to unauthorized access and/or acquisition due to Defendant's negligent and/or careless acts and omissions and its failure to protect said information.

13. In addition to Defendant's failure to prevent the breach, Defendant delayed several months before reporting said breach to the relevant governmental authorities and the affected individuals. As a result, Plaintiff and Class Members had no idea that such sensitive personal and familial information was compromised. As such, they were, and continue to be, at significant risk of identity theft and additional forms of personal, social, and financial harm.

14. Plaintiff brings this action on behalf of all persons whose PII was accessed, acquired, and/or misappropriated because of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) avoid sharing the PII of Plaintiff and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes.

15. Plaintiff and Class Members have suffered injury because of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual

consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

16. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use.

17. Defendant has a duty to safeguard and protect PII entrusted to it and could have prevented this theft had it limited the customer information received from its business associates and employed reasonable measures to ensure its systems were secure from threats like ransomware attacks.

18. Consequently, the PII of Plaintiff and Class Members was accessed and/or acquired by an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

19. Plaintiff Liam Murray was honorably discharged from the U.S. Marine Corps in November of 2022 and resides in New York County. Mr. Murray brings this action on behalf of himself, and others similarly situated.

20. Defendant OneTouchPoint, Inc. is a corporation organized under the laws of Delaware and its headquarters and principal place of business is located at 1225 Walnut Ridge Drive, Hartland, WI 53029.

21. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

22. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents, and/or assigns.

JURISDICTION AND VENUE

23. This Court has original jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2). The amount in controversy in this action exceeds $5,000,000, exclusive of interest and costs, and there are more than 100 members of the Class, defined below, many of which are citizens of a different state than Defendant. Defendant is a citizen of Wisconsin, where it maintains its principal place of business. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367.

24. This Court has personal jurisdiction over Defendant because Defendant has sufficient minimum contacts with this District and has purposely availed itself of the privilege of doing business in this district such that it could reasonably foresee litigation being brought in this District.

25. This Court also has diversity jurisdiction over this action pursuant to 28 U.S.C. § 1332(a)(1).

26. Venue is proper in this Court under 28 U.S.C. § 1391 because Defendant regularly transacts business in this District with consumers of New York state living in this district.

FACTUAL ALLEGATIONS

Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII

27. Defendant acquired, collected, and stored Plaintiff's and Class Members' PII.

28. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential personal and familial information. This PII contains static information that rarely, if ever, is changed including, but not limited to names, birthdates, sexes, Social Security numbers and demographic information. On information and belief, other highly sensitive information was subject to the breach including, but not limited to, subscriber ID numbers, diagnoses, medications, family histories, social histories, allergies, vitals, immunizations, and other information that was provided during health assessments.

29. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew, or should have known, that it was responsible for securing and protecting PII from disclosure.

30. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make or allow only authorized disclosures of this information.

Securing PII and Preventing Breaches

31. Defendant could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially years-old data from former customers.

32. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

33. Despite the prevalence of public announcements of data breach and data security compromises Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

34. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[9] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[10]

35. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

36. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit

[9] 17 CFR 248.201(b)(9) (2013).
[10] 17 CFR 248.201(b)(8)(i) (2013).
[11] Anita George, *Your Personal Data is For Sale on the Dark Web. Here's How Much It Costs,* DIGITAL TRENDS (Oct. 16, 2019), *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Dec. 21, 2022).

card number can sell for $5 to $110 on the dark web.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13]

37. As a result of Defendant's failure to properly secure Plaintiff's and the Class Members' PII, Plaintiff's and the Class Members' privacy has been invaded and all this personal information is likely for sale to criminals on the dark web. Consequently, unauthorized parties may have accessed and viewed Plaintiff's and the Class Members' unencrypted, non-redacted information, including name, contact and demographic information, date of birth, and healthcare information.

38. Given all the information obtained, the criminals would also be able to create numerous fake accounts and sell sensitive information, as part of their identity theft operation.

39. This high value data on the black market can be used to commit a myriad of financial crimes. Criminals seeking to engage in extremely specific targeted fraud schemes often use such PII to lend an air of legitimacy to their efforts to "phish" for information. PII can be used to "open new credit accounts on an ongoing basis rather than exploiting just one account until it's canceled" or "to access someone's financial records…making it possible to find and drain individuals' personal cash reserves."[14]

40. Further, among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

41. Stolen health data, like other PII, can be used to commit crimes like those above.

---

[12] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian.com, (Dec. 6, 2017), *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Dec. 21, 2022).

[13] *In the Dark*, VPN Overview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Dec. 21, 2022).

[14] Tim Greene, *Anthem Hack; Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, NETWORKWORLD (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Dec. 21, 2022).

However, this data is particularly useful for leveraging details specific of a disease or terminal illness in long-term identity theft. "Traditional criminals understand the power of coercion and extortion. By having healthcare information – specifically, regarding a sexually transmitted disease or terminal illness – that information can be used to extort or coerce someone to do what you want them to do".[15]

42. Plaintiff and Class Members are now subject to what has been referred to as "the privacy crime that can kill". PII pertaining to healthcare allows access to victim's medical insurance information which can be used to obtain free medical care. This could ruin credit and take years to resolve. Bad actors could max out victim's health policy limits leaving them without the means to pay for care. "Even worse, thieves might alter personal medical records including blood type, allergies or medicine, which could have a potentially fatal outcome."[16]

43. Plaintiff's and Class Members PII can be used in long-term scams like tax fraud and home equity loan fraud. As one Security executive stated, "[i]t's quite lucrative…and important for cybercriminals to have all the various identifying information about someone that is held in the records associated with health."[17]

44. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because credit and debit card accounts can be closed. The information compromised here is impossible to "close" and difficult, if not impossible, to change—name, contact information,

[15] Andre Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECHMAGAZINE, (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited Dec. 21, 2022).

[16] Laurie Zabel, *The Value of Personal Medical Information: Protecting Against Data Breaches*, NAHAM CONNECTIONS, https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information (last visited Dec. 21, 2022).

[17] Steger, *What Happens to Stolen Healthcare Data?* HEALTHTECHMAGAZINE (Oct. 30, 2019).

demographic information, and troves of personal information related to health and medical care.

45. PII containing health information is also sold by bad actors to traditional companies. Businesses benefit by leveraging information on diseases, conditions, and medications to create targeted marketing to potential consumers.[18]

46. The PII of Plaintiff and Class Members was taken by hackers to ultimately engage in identity theft. The fraudulent activity resulting from the Data Breach may not come to light for years.

47. There may be a lag between the time when harm occurs versus when it is discovered, i.e., when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [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.[19]

48. Plaintiff and Class Members face years of constant surveillance of their personal and financial records, the necessity of consistent monitoring of accounts, and loss of rights due to Defendant's failure to implement and maintain adequate data security protections and to prevent the intrusion and access by nefarious actors.

Defendant Failed to Comply with Statutory, Regulatory and Industry Standards

49. Due to the value of PII to bad actors, companies in the business of using, obtaining, storing, maintaining, and securing PII like Defendant are particularly vulnerable to

[18] Zabel, *The Value of Personal Medical Information: Protecting Against Data Breaches*. NAHAMCONNECTIONS (last visited Dec. 21, 2022).

[19] U.S. GEN. ACCOUNTABILITY OFFICE, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION, at 29 (June 2007), *available at:* https://www.gao.gov/products/gao-07-737 (last visited Dec.21, 2022).

cyber-attacks. Cybersecurity analysts have promulgated a series of best practices focusing on network security, facility security, and human resources security measures that should be implemented by businesses including, but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; data encryption; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system, and training staff regarding critical points and restricting access to data.[20] Defendant failed to comply with industry standards for the maintenance and protection of Plaintiff's and Class Members' PII.

50. Defendant, as a HIPAA Covered Entity business associate, is obligated to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164 subparts A and E ("Standard 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. These established national standards for the security of health information.

51. Defendant is required by HIPAA to "comply with the applicable standards, implementation specifications, and requirements" as set by the Act "with respect to electronic protected health information of a covered entity". 45 C.F.R. § 164.302. Defendant, thus, has a duty to secure Plaintiff's and Class member's PHI by ensuring its confidentiality and protecting against any reasonably anticipated threats, hazards, and unauthorized disclosures.

[20] James Edmondson, *5 Essential Data Security Best Practices for Keeping Your Data Safe*, BUSINESSTECHWEEKLY (Sept. 10, 2021), https://www.businesstechweekly.com/cybersecurity/data-security/5-essential-data-security-best-practices-for-keeping-your-data-safe/ (last visited Dec.21, 2022). See also, *Addressing BPO Information Security: A Three-Front Approach,* DATAMARK, Inc. (Nov. 2016) https://perma.cc/NY6X-TFUY (last visited Dec.21, 2022).

52. Defendant failed to implement appropriate security measures that would ensure the confidentiality of Plaintiff's and Class Members' PHI and protect it from the reasonably anticipated threat to its security by the unauthorized access and disclosure by bad actors.

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

54. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight 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.[21]

55. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[22] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

56. The FTC further recommends that companies not maintain PII longer than is

[21] FEDERAL TRADE COMMISSION, START WITH SECURITY: A GUIDE FOR BUSINESS, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Dec.21, 2022).

[22] FEDERAL TRADE COMMISSION, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Dec.21, 2022).

needed for authorization of a transaction; limit access to private 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.[23]

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

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

59. Defendants have obligations under other federal and state laws, regulations, contracts, and common law to maintain reasonable and appropriate physical, administrative, and electronic and technical measures to keep Plaintiff's and Class Members' PII confidential and to protect it from unauthorized access or disclosure.

60. Given the magnitude of the risk and potential ramifications of a data breach or attack, Defendant should have taken every reasonable measure to protect the PII of Plaintiff and Class Members, yet they failed to do so.

[23] FTC, START WITH SECURITY, supra.

Plaintiff and Class Members Suffered Damages

61. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including, but not limited to, Social Security numbers, dates of birth, and confidential health information. Defendant knew, or should have known, the foreseeable consequences that would occur if the PII was compromised, including the significant costs that would be imposed on Plaintiff and Class Members as a result.

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

63. Defendant was, or should have been, fully aware of the unique type and the significant volume of data stored on and/or shared on its system, amounting to hundreds of thousands of individuals' detailed personal and health information and, thus, the significant number of people who would be harmed by the exposure of the unencrypted data.

64. Defendant's notice of Data Breach was not just untimely but woefully deficient, failing to provide basic details, including but not limited to, how unauthorized parties accessed its networks, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach occurred system-wide, and what servers storing information were accessed.

65. The offered "advice" from Defendant is insufficient to protect Plaintiff and Class Members from the lifelong implications of having their most private PII accessed, acquired, exfiltrated, and/or published on the internet.

66. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of

Plaintiff and Class Members.

CLASS ALLEGATIONS

67. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

68. Plaintiff brings this Nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, and other applicable law.

69. Specifically, Plaintiff proposes the following Nationwide Class that Plaintiff seeks to represent be defined as follows:

> All Nationwide residents whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Cybersecurity Incident that Defendant published to Plaintiff and other Class Members on or around September 2, 2022.

70. The New York Subclass that Plaintiff seeks to represent is defined as follows:

> All New York residents whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Cybersecurity Incident that Defendant published to Plaintiff and other Class Members on or around September 2, 2022.

71. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff members.

72. Plaintiff reserves the right to modify or amend the definition of the proposed class and subclass before the Court determines whether certification is appropriate.

73. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant class-wide relief because Plaintiff and Class Members were subjected to the same wrongful practices by Defendant, entitling them to the same relief.

74. **Numerosity: Federal Rule of Civil Procedure 23(a)(1)**: The Nationwide Class and New York Subclass is so numerous that individual joinder of its members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, Plaintiff is informed and believes that there are thousands of Class Members. Those individuals' names and addresses are available from Defendant's records, and Nationwide Class Members and New York Subclass members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

75. **Commonality: Fed. R. Civ. P. 23(a)(2) and (b)(3)**: Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, common questions of law and fact exist as to members of the Nationwide Class and New York Subclass and predominate over any questions which affect only individual members of the Class. These common questions include, but are not limited to:

a. Whether Defendant had a duty to protect the confidentiality of Plaintiff's and Class Members' PII and prevent its disclosure, misappropriation, dissemination or misuse by authorized third parties;

b. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

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

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

e. Whether Defendant properly implemented its purported security measures to protect Plaintiff's and Class Members' PII from unauthorized capture, dissemination, and misuse;

f. Whether Defendant had a duty not to use the PII of Plaintiff and Class Members for non-business purposes;

g. Whether and when Defendant actually learned of the Data Breach and the extent thereof;

h. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

i. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

j. 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;

k. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

l. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

m. Whether Defendant willfully, recklessly, or negligently failed to implement, maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class Members' PII;

n. Whether Defendant was unjustly enriched by its actions; and

o. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages, restitution, injunctive relief, or other equitable relief, and the measure of such damages and relief.

76. **Typicality: Fed. R. Civ. P. 23(a)(3):** Consistent with Rule 23(a)(3), Plaintiff is a member of the Class he seeks to represent, and his claims and injuries are typical of the claims and injuries of the other Class Members. Plaintiff's PII was in Defendant's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to other Class Members and Plaintiff seek relief consistent with the relief of the Class.

77. **Adequacy: Fed. R. Civ. P. 23(a)(4):** Consistent with Rule 23(a)(4), Plaintiff will adequately and fairly protect the interests of other Class Members. Plaintiff has no interests adverse to the interests of absent Class Members. Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Defendant 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 and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

78. **Predominance & Superiority: Fed. R. Civ. P. 23(b)(3)**: Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient

adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

79. **Injunctive and Declaratory Relief**. Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant has acted or refused to act on grounds that apply generally to the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiff seeks prospective injunctive relief as a wholly separate remedy from any monetary relief.

80. Likewise, particular issues under Rule 23(c)(4) 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. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, and safeguarding their PII.

b. Whether Defendant failed to take commercially reasonable steps to safeguard the PII of Plaintiff and the Class Members.

c. Whether Defendant failed to adequately monitor and audit its data security systems that stored PII.

d. Whether adherence to FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

81. **Class Actions are Fiscally Responsible and Equitable**: A class action is superior to other available means for fair and efficient adjudication of the claims of the Class and would be beneficial for the parties and the court. Class action treatment will allow a large number of similarly situated persons to prosecute their common claims in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would require. The amounts owed to the many individual Class Members are likely to be relatively small, and the burden and expense of individual litigation would make it difficult or impossible for individual members of the class to seek and obtain relief. A class action will serve an important public interest by permitting such individuals to effectively pursue recovery of the sums owed to them.

82. **Risk of Prosecuting Separate Actions**: This case is appropriate for certification because class action litigation prevents the potential for inconsistent or contradictory judgments raised by individual litigation. Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

COUNT I

NEGLIGENCE
(On behalf of Plaintiff and Nationwide Class Members)

83. Plaintiff and the Nationwide Class reallege and incorporate by reference all preceding paragraphs as if set fully herein.

84. Plaintiff and the Nationwide Class entrusted their PII to Defendant and/or their medical providers and/or insurance carriers with certain PII including but not limited to names, dates of birth, addresses, and information collected during health assessments with the understanding that their PII and its confidentiality would be protected from unauthorized disclosure or misappropriation.

85. Defendant accepted and stored the PII of Plaintiff and the Nationwide Class in its computer systems and on its networks. Upon doing so, Defendant undertook and owed a duty of care to Plaintiff and Nationwide Class to adequately secure and safeguard that PII and its confidentiality.

86. Defendant has full knowledge of the sensitive nature of said PII and the types of harm that could befall Plaintiff and Nationwide Class if wrongfully accessed or disclosed.

87. Defendant knew or reasonably should have known the failure to exercise care in the collection, storage, control or use of said PII involved an unreasonable risk of harm to Plaintiff and Nationwide Class even if that harm occurred through the criminal activity of a third party.

88. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing

Defendant's security protocols to ensure that the PII of Plaintiff and the Nationwide Class in Defendant's possession was adequately secured and protected.

89. Defendant had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain pursuant to contractual obligations or state and federal regulations, including that of former customers.

90. Defendant also had a duty implement processes to detect and prevent the improper access and misuse of the PII of Plaintiff and the Nationwide Class.

91. Defendant was subject to an "independent duty" untethered to any contract between Defendant and Plaintiff and the Nationwide Class.

92. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in receiving, collecting and storing the PII of Plaintiff and Class Members, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

93. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Nationwide Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and Nationwide Class Members, including basic encryption techniques freely available to Defendant.

94. Plaintiff and Nationwide Class Members had no ability to protect their PII that was, and possibly remains, in Defendant's possession.

95. Defendant was in a position to protect against the harm suffered by Plaintiff and the Nationwide Class that was a result of the Data Breach.

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

97. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Nationwide Class Members.

98. Defendant has admitted that the PII of Plaintiff and the Nationwide Class was wrongfully accessed by, disclosed to, and/or acquired by unauthorized third persons as a result of the Data Breach.

99. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Nationwide Class during the time the PII was within Defendant's possession or control.

100. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

101. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Nationwide Class in the face of increased risk of theft.

102. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of their PII.

103. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII it was no longer required to retain pursuant to regulations.

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

105. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and the Nationwide Class would not have been compromised.

106. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and Nationwide Class. Their PII was compromised as the proximate result of Defendant's failure to exercise reasonable care in safeguarding the PII by adopting, implementing, and maintaining appropriate security measures.

107. Additionally, § 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 Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

108. Defendant violated § 5 of the FTC Act by failing to use reasonable measures to protect PII and failing to comply with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the

foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

109. Defendant's violation of § 5 of the FTC Act constitutes negligence *per se.*

110. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

111. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

112. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the 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, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and Class Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII

compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

113. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Nationwide Class 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.

114. Additionally, as a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

115. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT II
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

116. Plaintiff fully incorporates by reference all the above paragraphs as though fully set forth herein.

117. Defendant contracted to provide services to Plaintiff's and the Nationwide Class's respective medical providers.

118. These contracts were made expressly for the benefit of Plaintiff and the Nationwide Class in that it was their confidential PII including medical information that Defendant agreed to receive, collect, use and protect while providing its services. The benefit of the receipt, collection, use and protection of this PII was the direct and primary objective of the contracting parties.

119. Defendant knew that breach of these customer contracts would cause harm to its customers' patients and/or clients (Plaintiff and Nationwide Class members) including, but not limited to, identity theft and fraud.

120. Defendant breached its contracts with its customers who were affected by the Data Breach when it failed to adequately secure and protect the PII of Plaintiff and Nationwide Class members, when it failed to use reasonable data security measures that could have prevented this Breach and when it failed to notify its customers in a timely manner that the data entrusted to Defendant had been accessed, compromised, and/or stolen.

121. As a result of Defendant's breach, Plaintiff and the Nationwide Class are entitled to damages in an amount to be determined at trial along with their costs and attorney fees incurred in this action.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and Nationwide Class)

122. Plaintiff fully incorporates by reference all the above paragraphs as though fully set forth herein.

123. Defendant solicited and invited Plaintiff and the Nationwide Class to provide their PII to Defendant, either directly or indirectly through Defendant's customers, the Covered Entities, as part of Defendant's regular business practices. Plaintiff and the Nationwide Class accepted Defendant's offers and provided their PII to Defendant.

124. For its business use, Defendant collected and maintained the PII entrusted by Plaintiff and the Nationwide Class to their medical providers and/or insurance carriers. In so doing, Plaintiff and the Nationwide Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Nationwide Class if their data had been breached and compromised or stolen.

125. A meeting of the minds occurred when Plaintiff and the Nationwide Class agreed to, and did, provide their PII to Defendant and/or Defendant's customers, in exchange for, among other things, the protection of their PII.

126. Plaintiff and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

127. Defendant breached the implied contracts it made with Plaintiff and the Nationwide Class by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

128. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Nationwide Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports, insurance statements and medical records; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

129. As a result of Defendant's breach of implied contract, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT IV
INVASION OF PRIVACY
(On Behalf of Plaintiff and Nationwide Class Members)

130. Plaintiff and the Nationwide Class reallege and incorporate all prior paragraphs as though fully set forth herein.

131. Plaintiff and the Nationwide Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

132. Defendant owed a duty to its customers, including Plaintiff and Nationwide Class Members, to keep the PII entrusted to it and contained within its systems confidential.

133. Defendant failed to protect and allowed access to and/or released to unknown and unauthorized third parties the PII of Plaintiff and Nationwide Class Members.

134. Defendant allowed unauthorized and unknown third parties to access and examine the PII of Plaintiff and Nationwide Class Members, by way of Defendant's failure to protect the PII.

135. The unauthorized release to, custody of, and/or examination by unauthorized third parties of the PII of Plaintiff and the Nationwide Class is highly offensive to a reasonable person.

136. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Nationwide Class disclosed their PII to Defendant through their respective relationships with their medical providers and/or insurance carrier, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

137. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

138. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

139. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

140. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and the Nationwide Class was disclosed to third parties without authorization, causing Plaintiff and the Nationwide Class to suffer damages.

141. Plaintiff and Class Members seek equitable relief to prevent and restrain the ongoing and future invasions of their privacy and compensatory damages for the harm Class members have suffered as a result of the Data Breach.

COUNT V
VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 349
(On Behalf of Plaintiff and New York Subclass)

142. Plaintiff brings this claim on behalf of himself and the New York Subclass [hereinafter "Subclass].

143. Plaintiff and the Subclass reallege and incorporate all preceding paragraphs as if fully set forth herein.

144. Plaintiff and Subclass are persons within the meaning of New York General Business Law ["GBL"] § 349(h).

145. GBL § 349(a) prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state". Defendant engaged in deceptive acts and practices in the form of misrepresentation and omissions during the conduct of business in New York by engaging in the methods, acts, practices, and conduct described in the Complaint, including but not limited to (i) establishing the sub-standard security practices and procedures described herein; (ii) soliciting and collecting the PII of Plaintiff and Subclass with the knowledge that the information would not be adequately protected; (iii) storing Plaintiff's and Subclass members' PII in an unsecure environment and failing to take reasonable methods to safeguard said PII; (iv) making false, misleading, deceptive and/or inaccurate statements and/or

omitting material information concerning Defendant's security measures, expertise, and vigilance in the care and handling of the PII entrusted by Plaintiff and Subclass members; (v) engaging in unlawful acts and practices by failing to disclose the Data Breach to Subclass members in a timely and accurate manner.

146. By engaging in the above acts and practices, Defendant committed an "unlawful act or practice" within the meaning of § 349 of the GBL. Plaintiffs and Subclass members suffered substantial injury they could not reasonably have avoided other than by refraining from seeking medical care, being uninsured and/or failing to provide a true and accurate personal or family medical history and other PII to their medical providers.

147. Defendant's violations of GBL § 349 have directly, foreseeably, and proximately caused damages and injury to Plaintiff and Subclass. Plaintiff and Subclass relied on and made provider decisions based wholly or in part on Defendant's and its customers representations regarding its security measures and trusted that Defendant would keep their PII safe and secure. Accordingly, Plaintiff and Subclass provided their PII with the reasonable belief and expectation that it would be safe, private, and secure and any mishap would be handled expediently, expertly, and with full disclosure of the material facts to any party injured by a breach or attempt thereof – something Defendant failed to do in a timely and adequate manner.

148. Defendant knew or should have known that Defendant's system of information storage and data security measures were inadequate to safeguard the vital PII provided by Plaintiff and Subclass members. Defendant knew or should have known that the risk of breach or theft was highly likely given repeated government and security expert public warnings. Defendant's actions engaging in the above-described unlawful practices and acts were negligent at best. At worst, they

were a knowing, willful and/or wanton and reckless disregard to the rights of Plaintiff and Subclass.

149. Plaintiff and Subclass members seek relief under New York GBL § 349 including but not limited to, restitution for money or other financial benefit that Defendant may have acquired by means of Defendant's unlawful acts or practices, damages and restitution for actual losses "or fifty dollars, whichever is greater" suffered as a result of said unlawful acts and practices, declaratory relief, and attorneys' fees and costs. Additionally, Plaintiff and Subclass seek treble damages under § 349(h) which provides for the award of damages "to an amount not to exceed three times the actual damages up to one thousand dollars, if the court finds the defendant willfully or knowingly violated this section."

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself, Nationwide Class, and Subclass Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and appointing Plaintiff and their counsel to represent such Class;

B. For an Order certifying the New York State Class and appointing Plaintiff and their Counsel to represent such Class;

C. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including

but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and the Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

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

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any

new or modified procedures;

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

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employee's compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all the Nationwide Class and New

York State Class about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

E. For an award of damages, including actual, consequential, nominal, and statutory damages, as allowed by law in an amount to be determined;

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

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: January 12, 2023

THE LAW OFFICE OF PAUL C. WHALEN, P.C.

/s/Paul C. Whalen

PAUL C. WHALEN, ESQ.
[PW1300]
768 Plandome Road
Manhasset, NY 11030
(516) 426-6870
pcwhalen@gmail.com

Attorney for Plaintiff and the Putative Class