UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF WISCONSIN

RICHARD KREFTING, individually and on behalf of all others similarly situated, Plaintiff, v. ONETOUCHPOINT, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Richard Krefting ("Plaintiff"), individually and on behalf of all other similarly situated individuals (the "Class Members," as defined below), by and through counsel, file this Class Action Complaint against OneTouchPoint, Inc. ("OneTouchPoint" or "Defendant") and allege the following based on personal knowledge of facts pertaining to his and on information and belief based on the investigation of counsel as to all other matters.

I. NATURE OF THE ACTION

1. OneTouchPoint provides printing and mailing services for numerous companies across the United States. For business purposes, Defendant received the information of individuals from customer organizations which Defendant utilized to conduct mailings on behalf of their customers.[1]

[1] *See* https://ago.vermont.gov/blog/2022/07/27/onetouchpoint-data-breach-notice-to-consumers/*; see also* https://1touchpoint.com/services.

2. Plaintiff and the Class Members (as further defined below) have had their personal identifiable information exposed as a result of OneTouchPoint's inadequately secured computer network. Defendant betrayed the trust of Plaintiff and the other Class Members by failing to properly safeguard and protect their personal identifiable information and thereby enabling cybercriminals to steal such valuable and sensitive information.

3. This class action seeks to redress OneTouchPoint's unlawful, willful and wanton failure to protect the personal identifiable information of the 2,651,396 individuals that was exposed in a major data breach of Defendant's network (the "Data Breach" or "Breach"), in violation of its legal obligations.[2]

4. The Data Breach was discovered on April 28, 2022, when OneTouchPoint learned that a cyberattack had been successfully launched on its systems.[3] OneTouchPoint investigated the attack with the assistance of third-party computer specialists. OneTouchPoint provided a summary of the investigation to its customers beginning on June 3, 2022.[4] The forensic investigation determined that cybercriminals gained unauthorized access to certain systems containing the personal identifiable information of 2,651,396 individuals.[5]

5. According to OneTouchPoint and information provided by its affected customers, the personal identifiable information exposed in the Breach included: names, addresses, Social Security numbers, account numbers, credit score, ("PII") and medical information ("PHI") (collectively "Private Information").[6]

---

[2] https://apps.web.maine.gov/online/aeviewer/ME/40/d90babd7-ded0-457b-8a6e-66360be5c9cc.shtml.

[3] *See* https://ago.vermont.gov/blog/2022/07/27/onetouchpoint-data-breach-notice-to-consumers/.

[4] *Id.*

[5] *Id.*; *see also* https://apps.web.maine.gov/online/aeviewer/ME/40/d90babd7-ded0-457b-8a6e-66360be5c9cc.shtml.

[6] *Id.*; *see also* Plaintiff's breach notification letter, attached as Exhibit 1.

6. Due to Defendant's negligence, cybercriminals obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of hundreds of thousands of individuals.

7. For the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Plaintiff and Class Members will have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their of Private Information, and/or additional damages as described below.

8. Plaintiff brings this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

Plaintiff

9. Plaintiff Richard Krefting is domiciled in and a citizen of the state of Washington.

10. On or around July 25, 2022, Plaintiff received a breach notification letter from informing him that his personal information, including name, address, account number(s), credit score, and Social Security number had been exposed to cybercriminals during the Data Breach.[7]

[7] Upon information and belief, OneTouchPoint is the "printing vendor" referenced in the BECU breach notification letter. This is supported, among other things, by the similar timing and information provided by Defendant.

Defendant

11. Defendant OneTouchPoint is a Wisconsin corporation with its principal place of business in Hartland, Wisconsin.

12. OneTouchPoint provides printing and mailing services for numerous companies across the United States. For business purposes, Defendant received the information of individuals from customer organizations which Defendant utilized to conduct mailings on behalf of their customers.[8]

III. JURISDICTION AND VENUE

13. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

14. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, it regularly transacts business in this District, and many Class Members reside in this District. Venue is likewise proper as to Defendant in this District because Defendant employs a significant number of Class Members in this District, and a substantial part of the events or omissions giving rise to the claim occurred in this District. 28 U.S.C. § 1391(b)(2).

IV. FACTUAL ALLEGATIONS

A. The Data Breach

15. Based on information supplied by Defendant, the Data Breach was discovered on April 28, 2022, when OneTouchPoint learned that a cyberattack had been successfully launched

[8] *See* https://ago.vermont.gov/blog/2022/07/27/onetouchpoint-data-breach-notice-to-consumers/*; see also* https://1touchpoint.com/services.

on its systems.[9] OneTouchPoint investigated the attack with the assistance of third-party computer specialists. OneTouchPoint provided a summary of the investigation to its customers beginning on June 3, 2022.[10] The forensic investigation determined that cybercriminals gained unauthorized access to certain systems containing the personal identifiable information of 2,651,396 individuals.[11]

16. According to OneTouchPoint and information provided by its affected customers, the personal identifiable information exposed in the Breach included: names, addresses, Social Security numbers, account numbers, credit score, and medical information.[12]

17. Defendant failed to take the necessary precautions required to safeguard and protect Plaintiff's and the other Class Members' Private Information from unauthorized disclosure. Defendant's actions represent a flagrant disregard of the rights of the Class Members, both as to privacy and property.

B. Plaintiff's Experiences

18. On or around July 25, 2022, Plaintiff received a breach notification letter from Boeing Employees' Credit Union ("BECU") informing him that his personal information, including name, address, account number(s), credit score, and Social Security number had been exposed to cybercriminals during the Data Breach.[13] Upon information and belief,

[9] *See* https://ago.vermont.gov/blog/2022/07/27/onetouchpoint-data-breach-notice-to-consumers/.

[10] *Id.*

[11] *Id.*; *see also* https://apps.web.maine.gov/online/aeviewer/ME/40/d90babd7-ded0-457b-8a6e-66360be5c9cc.shtml.

[12] *Id.*; *see also* Plaintiff's breach notification letter, attached as Exhibit 1.

[13] This is supported, among other things, by the similar timing and information provided by Defendant.

OneTouchPoint is the "printing vendor" referenced in the BECU breach notification letter. The letter Plaintiff received is attached as Exhibit 1 hereto.

19. Plaintiff and Class Members' Private Information was entrusted to Defendant for employment opportunities with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

20. Because of the Data Breach, Plaintiff's Private Information is now in the hands of cyber criminals. Plaintiff and all Class Members are now imminently at risk of crippling future identity theft and fraud.

21. Plaintiff has already experienced identity theft. Indeed, following the Data Breach, Plaintiff has discovered a credit account fraudulently opened using his personal information. Additionally, since the Data Breach, Plaintiff has received notification from Credit Karma that someone has attempted to change the location of his home address.

22. As a result of the Data Breach, Plaintiff has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff has spent time researching the facts and scope of the Data Breach, monitoring his accounts and personal information, reviewing his credit reports, responding to the fraudulent activity his already experienced, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach.

23. As a direct and proximate result of the Data Breach, Plaintiff will likely need to purchase a lifetime subscription for identity theft protection and credit monitoring.

24. Plaintiff has been careful to protect and monitor his identity.

25. Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and

certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cybercriminals; (c) damages to and diminution in value of Plaintiff's Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's Private Information; and (e) continued risk to Plaintiff's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

C. Cybercriminals Have Used and Will Continue to Use Plaintiff's Private Information to Defraud Them

26. Private Information of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety sordid ways for criminals to exploit Plaintiff and the Class Members and to profit off their misfortune.

27. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[14] For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government

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

benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[15] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

28. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[16]
>
> [Emphasis added.]

29. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[17]

30. This was a financially motivated Breach, as the only reason the cyber criminals go through the trouble of running a targeted cyberattack against companies like OneTouchPoint is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[18] "[I]f there is reason to believe that your

---

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

[16] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[17] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

[18] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

personal information has been stolen, you should assume that it can end up for sale on the dark web."[19]

31. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, they ***will*** use it.[20]

32. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

33. For instance, with a stolen social security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[22]

34. The medical information, PHI, that was exposed is also highly valuable. PHI (which stands for protected health information) can sell for as much as $363 according to the Infosec Institute.[23]

---

[19] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[20] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[21] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

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

[23] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at:* https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/.

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

36. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[24]

37. The ramifications of Defendants' failure to keep its Class Members' Private Information secure are long lasting and severe. Once that information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

38. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

39. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened. [25] This gives thieves ample time to seek multiple

[24] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.

[25] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2.

treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[26]

40. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[27]

41. As a direct and proximate result of the Data Breach, Plaintiff and the Class have had their Private Information exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of further harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, following Federal Trade Commission checklists, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps.

42. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;

---

[26] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages"), available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[27] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

b. Trespass, damage to, and theft of their personal property including Private Information;

c. Improper disclosure of their Private Information;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and having been already misused;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their Private Information and that identity thieves have already used that information to defraud other victims of the Data Breach;

f. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

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

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

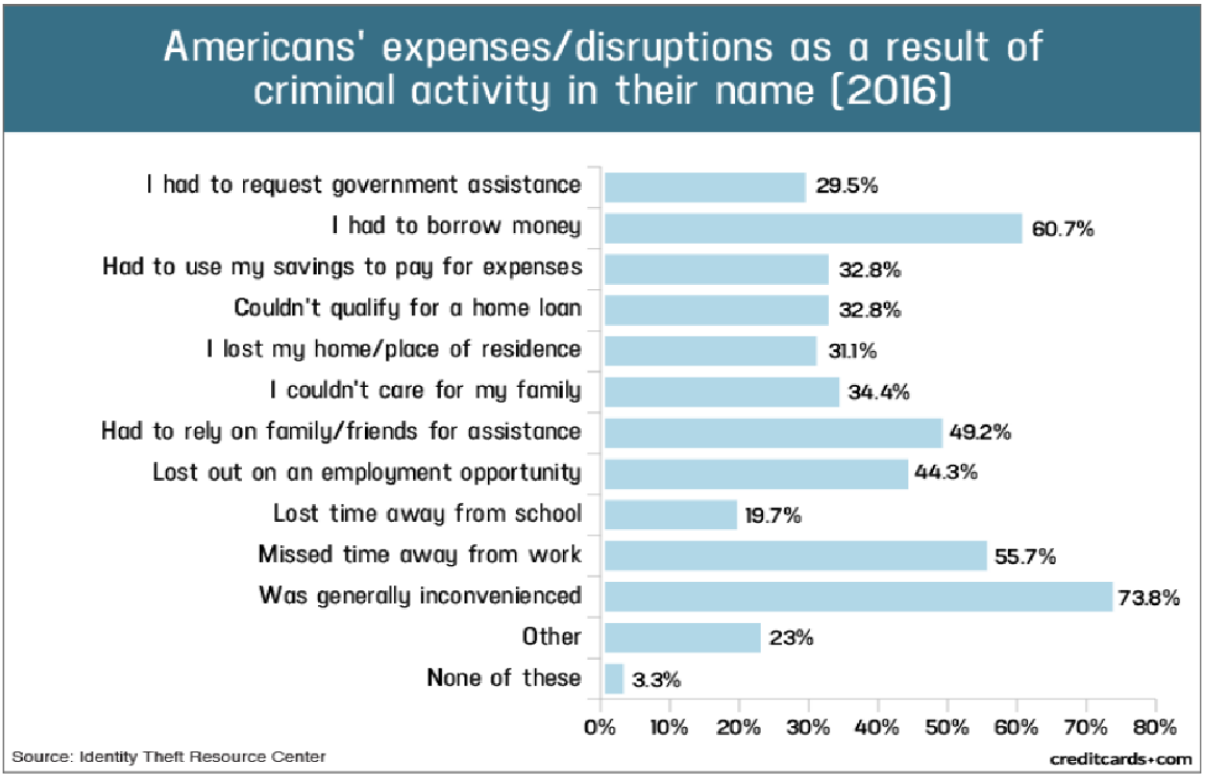
i. The loss of use of and access to their credit, accounts, and/or funds;

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

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

43. Below is a chart that shows the kinds of expenses and disruptions that victims of identity theft experience[28]:

[28] Jason Steele, *Credit Card and ID Theft Statistics*, CREDITCARDS.COM (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.



44. Moreover, Plaintiff and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiff's Private Information.

45. Plaintiff and Class Members also have an interest in ensuring that their personal information that was provided to OneTouchPoint is removed from OneTouchPoint's unencrypted files.

46. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiff and Class Members the inadequate 24 months of identity theft repair and monitoring services. This limited identity theft monitoring is, however, inadequate to protect Plaintiff and Class Members from a lifetime of identity theft risk.[29]

[29] *See* Exhibit 1, attached hereto.

47. Defendant further acknowledged, in its letter to Plaintiff and other Class Members, that, in response to the Data Breach, OneTouchPoint "worked with our experts to try to prevent such an incident from ever happening again."[30]

48. The letter further acknowledged that the Data Breach would cause inconvenience to affected individuals by providing numerous "steps" for Class Members to take in an attempt to mitigate the harm caused by the Data Breach.[31] and that financial harm would likely occur, stating: "We are notifying potentially impacted individuals, including you, so that you may take steps to protect your information…. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

49. At OneTouchPoint's suggestion, Plaintiff is desperately trying to mitigate the damage that OneTouchPoint has caused him. Given the kind of Private Information OneTouchPoint made accessible to hackers, however, Plaintiff is certain to incur additional damages. Because identity thieves have his Private Information, Plaintiff and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[32]

50. None of this should have happened.

---

[30] *Id.*

[31] *Id.*

[32] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

D. Defendant was Aware of the Risk of Cyber Attacks

51. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[33] Yahoo,[34] Marriott International,[35] Chipotle, Chili's, Arby's,[36] and others.[37]

52. Companies providing services to the healthcare industry, such as OneTouchPoint, have been prime targets for cyberattacks. As early as August 2014, the FBI specifically warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[38] Here, as Defendant explained in the letter it sent to Plaintiff, OneTouchPoint "process[es] information for health plans[.]" Based on information obtained by Plaintiff, OneTouchPoint processes health information for major insurance companies, including Blue Cross Blue Shield of Michigan.

---

[33] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[34] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[35] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[36] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[37] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[38] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

53. OneTouchPoint should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the Private Information that it collected and maintained.

54. Indeed, OneTouchPoint's Privacy Policy states the following:

> The Company takes the privacy and security of individuals and their personal information very seriously, and we take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorized access, alteration, disclosure or destruction and have several layers of security measures, including:
>
> - Encryption using certificates from trusted certificate authorities
> - Security by design
> - Edge and internal firewalls to segregate roles
> - Segregation of datasets
> - Physical and digital access controls
> - A complex passphrase policy
> - Off-site backups
> - Regular patch cycle and reporting
> - Regular penetration and vulnerability testing by external specialists[39]

55. OneTouchPoint's assurances of maintaining high standards of cybersecurity make it evident that OneTouchPoint recognized it had a duty to use reasonable measures to protect the Private Information that it collected and maintained. Yet, it appears that OneTouchPoint did not meaningfully or comprehensively use the reasonable measures, including the measures it claims to utilize.

[39] *See* https://www.morleynet.com/About/Privacy-Policy/ (last visited February 28, 2022).

56. OneTouchPoint was clearly aware of the risks it was taking and the harm that could result from inadequate data security.

E. OneTouchPoint Could Have Prevented the Data Breach

57. Data breaches are preventable.[40] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[41] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[42]

58. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[43]

59. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[44] The guidelines

---

[40] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[41] *Id.* at 17.

[42] *Id.* at 28.

[43] *Id.*

[44] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

establish that businesses should protect the confidential 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 for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

60. Upon information and belief, OneTouchPoint failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, OneTouchPoint also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

61. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[45]

62. To prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

[45] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[46]

63. Further, to prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

[46] *Id.* at 3-4.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[47]

64. In addition, to prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**

  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials

- **Thoroughly investigate and remediate alerts**

  - Prioritize and treat commodity malware infections as potential full compromise;

- **Include IT Pros in security discussions**

  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**

  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**

  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**

  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection

[47] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001.

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[48]

65. Given that Defendant was storing the Confidential Information of more than 500,000 individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

66. Specifically, among other failures, OneTouchPoint had far too much confidential unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.[49] Indeed, the United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information, stating "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[50]

67. In sum, this Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all confidential information. Further, the Data Breach could have likely been prevented had Defendant utilized appropriate malware prevention and detection technologies.

F. Defendant's Response to the Data Breach is Inadequate to Protect Plaintiff and the Class

68. Defendant failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

---

[48] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

[49] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

[50] "Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

69. Defendant stated that it discovered the Data Breach in April 2022. And yet, OneTouchPoint did not start notifying affected individuals until July 2022—months after it learned of the Data Breach. Even then, OneTouchPoint failed to inform Plaintiff and Class Members exactly what information was exposed in the Data Breach, leaving Plaintiff and Class Members unsure as to the scope of information that was compromised.

70. During these intervals, the cybercriminals were exploiting the information while OneTouchPoint was secretly still investigating the Data Breach.

71. If OneTouchPoint had investigated the Data Breach more diligently and reported it sooner, Plaintiff and the Class could have taken steps to protect themselves sooner and to mitigate the damages caused by the Breach.

V. CLASS ACTION ALLEGATIONS

72. Plaintiff incorporates by reference all preceding paragraphs as if fully restated here.

73. Plaintiff brings this action against OneTouchPoint on behalf of themselves and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of a nationwide class and the state subclass (collectively, the "Class") defined as follows:

> Nationwide Class
> All persons whose Private Information was compromised as a result of the Data Breach.
>
> Washington Subclass
> All persons residing in Washington whose Private Information was compromised as a result of the Data Breach.

74. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors,

subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

75. Plaintiff reserves the right to amend the above definitions or to propose additional subclasses in subsequent pleadings and motions for class certification.

76. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

77. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. Defendant has reported that the total number of individuals affected in the Data Breach was 2,651,396 individuals.

78. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through OneTouchPoint's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive Private Information compromised in the same way by the same conduct of OneTouchPoint.

79. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

80. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the

Class individually to effectively redress OneTouchPoint's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

81. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's Private Information;

c. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their Private Information, and whether it breached this duty;

d. Whether OneTouchPoint breached its duties to Plaintiff and the Class as a result of the Data Breach;

e. Whether OneTouchPoint failed to provide adequate cyber security;

f. Whether OneTouchPoint knew or should have known that its computer and network security systems were vulnerable to cyber attacks;

g. Whether OneTouchPoint's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;

h. Whether OneTouchPoint was negligent in permitting unencrypted Private Information of vast numbers of individuals to be stored within its network;

i. Whether OneTouchPoint was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach to include former employees, applicants, and business associates;

j. Whether OneTouchPoint failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

k. Whether OneTouchPoint continues to breach duties to Plaintiff and the Class;

l. Whether Plaintiff and the Class suffered injury as a proximate result of OneTouchPoint's negligent actions or failures to act;

m. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

n. Whether OneTouchPoint's actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of all Plaintiffs and the Class)

82. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

83. Defendant OneTouchPoint solicited, gathered, and stored the Private Information of Plaintiff and the Class.

84. Defendant had full knowledge of the sensitivity of the Private Information it maintained and of the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiff and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their Private Information that was in OneTouchPoint's possession. As such, a special relationship existed between OneTouchPoint and Plaintiff and the Class.

85. Defendant was well aware of the fact that cybercriminals routinely target corporations, particularly those servicing the health industry, through cyberattacks in an attempt to steal the collected Private Information.

86. Defendant owed Plaintiff and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

87. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

88. Defendant had duties to protect and safeguard the Private Information of Plaintiff and the Class from being vulnerable to cyberattacks, including by encrypting documents

containing Private Information, by not permitting documents containing unencrypted Private Information to be maintained on its systems, and other similarly common-sense precautions when dealing with sensitive Private Information. Additional duties that OneTouchPoint owed Plaintiff and the Class include:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Private Information in its possession;
b. To protect the Private Information in its possession using reasonable and adequate security procedures and systems;
c. To adequately and properly audit and test its systems;
d. To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;
e. To train its employees not to store Private Information for longer than absolutely necessary;
f. To implement processes to quickly detect a data breach, security incident, or intrusion; and
g. To promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

89. Plaintiff and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and OneTouchPoint. Defendant was in a position to ensure that its systems were sufficient to protect the Private Information that Plaintiff and the Class had entrusted to it.

90. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' Private Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the Private Information in its possession;

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit and test its computer systems to avoid cyberattacks;

d. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information, including maintaining it in an encrypted format;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff and the Class's Private Information;

f. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

g. Failing to abide by reasonable retention and destruction policies for Private Information it collects and stores; and

h. Failing to promptly and accurately notify Plaintiff and Class Members of the Data Breach that affected their Private Information.

91. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

92. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

93. The damages Plaintiff and the Class have suffered (as alleged above) were and are reasonably foreseeable.

94. The damages Plaintiff and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

95. Plaintiff and the Class have suffered injury, including as described in Section IV.B, *supra*, and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of all Plaintiffs and the Class)

96. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

97. Through the use of Plaintiff's and Class Members' Private Information, Defendant received monetary benefits.

98. Defendant collected, maintained, and stored the Private Information of Plaintiff and Class Members and, as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiff and Class Members.

99. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members and accepted that monetary benefit.

100. However, acceptance of the benefit under the facts and circumstances described herein, make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures 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 data security.

101. Under the principle of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members because Defendant failed to implement the appropriate data management and security measures.

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

103. If Plaintiff and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to allow Defendant to have or maintain their Private Information.

104. As a direct and proximate result of Defendant's decision to profit rather than provide adequate data security, Plaintiff and Class members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Defendant reasonably should have expended on data security measures to secure Plaintiff's Private Information, (ii) time and expenses mitigating harms, (iii) diminished value of the Private Information, (iv) harms as a result of identity theft; and (v) an increased risk of future identity theft.

105. Defendant, upon information and belief, has therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiff and the Class in direct violation of Plaintiff's and Class members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

106. Accordingly, Plaintiff and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiff and the Class.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of all Plaintiffs and the Class)

107. Plaintiff incorporates by reference all allegations of the preceding factual allegations as though fully set forth herein.

108. Defendant required Plaintiff and Class Members to provide, or authorize the transfer of, their Private Information in order for Afni to provide services. In exchange, Defendant entered into implied contracts with Plaintiff and Class Members in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff's and Class members' Private Information and to timely notify them in the event of a data breach.

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

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

111. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

112. The losses and damages Plaintiff and Class members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class members.

FOURTH CAUSE OF ACTION
VIOLATIONS OF WISCONSIN'S DECEPTIVE TRADE PRACTICES ACT
(WIS. STAT. § 100.18, *ET SEQ*)
(On Behalf of all Plaintiffs and the Class)

113. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

114. Defendant's conduct violates Wisconsin's Deceptive Trade Practices Act, WIS. STAT. §100.18 (the "WDTPA"), which provides that no,

> firm, corporation or association, ... with intent to sell, distribute, increase the consumption of ... any ... merchandise ... directly or indirectly, to the public for sale... shall make, publish, disseminate, circulate, or place before the public ... in this state, in a ... label ... or in any other way similar or dissimilar to the foregoing, an advertisement, announcement, statement or representation of any kind to the public... which ... contains any assertion, representation or statement of fact which is untrue, deceptive or misleading.

115. Plaintiff and Class Members "suffered pecuniary loss because of a violation" of the WDTPA. WIS. STAT. §100.18(11)(b)(2).

116. Defendant violated the WDTPA by: (a) fraudulently advertising material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, to prevent infiltration of the security system so as to safeguard Private Information from unauthorized access; (b) misrepresenting material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, so as to safeguard Private Information from unauthorized access; (c) omitting, suppressing, and concealing the material fact of the inadequacy of the security practices and procedures; (d) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, to prevent infiltration of the security system so as to safeguard Private Information from unauthorized access; and (e) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action

to enact reasonable security practices to safeguard its systems and data from cyberattacks like the Data Breaches.

117. Defendant knew or should have known that its computer systems and security practices and procedures were inadequate and that risk of the Data Breaches and theft was high.

118. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class Members.

119. Plaintiff and the Class Members relied upon Defendant's deceptive and unlawful marketing practices and are entitled to damages, including reasonable attorney fees and costs, punitive damages, and other relief which the court deems proper. WIS. STAT. §§ 100.18(11)(b)(2) and 100.20(5).

FIFTH CAUSE OF ACTION
INJUNCTIVE AND DECLARATORY RELIEF
(On Behalf of Plaintiff and the Washington Subclass)

120. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

121. Defendant is a "person" within the meaning of the Washington Consumer Protection Act, RCW 19.86.010 and it conducts "trade" and "commerce" within the meaning of RCW 19.86.010(2).

122. Plaintiff and the Class are "persons" within the meaning of RCW 19.86.010(1).

123. Defendant engaged in unfair or deceptive acts or practices in the conduct of its business by through the conduct set forth throughout this Complaint. These unfair or deceptive acts or practices include, without limitation, the following:

a. Failing to adequately secure Plaintiff's and Class members' Private Information from disclosure to unauthorized third parties or for improper purposes;

b. Enabling the disclosure of Plaintiff's and Class members' Private Information in a manner highly offensive to a reasonable person;

c. Enabling the disclosure of Plaintiff's and Class members' Private Information without their informed, voluntary, affirmative, and clear consent;

d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' Private Information; and

e. Failing to disclose the Data Breach in a timely and accurate manner.

124. Defendant's systematic acts or practices are unfair because these acts or practices (1) caused substantial financial injury to Plaintiffs' and Class members; (2) are not outweighed by any countervailing benefits to consumers or competitors; and (3) are not reasonably avoidable by consumers.

125. Defendant's systematic acts or practices are unfair because the acts or practices are immoral, unethical, oppressive, and/or unscrupulous.

126. Defendant's systematic acts or practices are deceptive because they were, and are capable of, deceiving a substantial portion of the public.

127. Defendant's unfair and deceptive acts or practices have repeatedly occurred in trade or commerce within the meaning of RCW 19.86.010 and RCW 19.86.020.

128. The acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

129. Defendant's unfair or deceptive acts or practices impact the public interest because they have injured Plaintiffs and Class members.

130. As a direct and proximate result of Defendant's unfair or deceptive acts or practices, Plaintiffs and Class members have suffered injury in fact and lost money.

131. As a result of Defendant's conduct, Plaintiffs and Class members have suffered actual damages, including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased and imminent risk of fraud and identity theft, the lost value of their Private Information, and other economic and non-economic harm.

132. Plaintiff and the Class are therefore entitled to legal relief against Defendant, including recovery of nominal damages, actual damages, treble damages, injunctive relief, attorneys' fees and costs, and such further relief as the Court may deem proper.

133. Plaintiff and the Class are also entitled to injunctive relief in the form of an order prohibiting Defendant from engaging in the alleged misconduct and such other equitable relief as the Court deems appropriate.

SIXTH CAUSE OF ACTION
INJUNCTIVE AND DECLARATORY RELIEF
(On Behalf of all Plaintiffs and the Class)

134. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

135. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

136. As previously alleged and pleaded, Defendant owes duties of care to Plaintiff and Class Members that requires it to adequately secure their Private Information.

137. Defendant still possesses the Private Information of Plaintiff and the Class Members.

138. Defendant has not satisfied its obligations and legal duties to Plaintiff and the Class Members.

139. Defendant has claimed that it is taking some steps to increase its data security, but there is nothing to prevent Defendant from reversing these changes once it has weathered the increased public attention resulting from this Breach, and to once again place profits above protection.

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

a. Ordering Defendant to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
b. Ordering Defendant to significantly increase its spending on cybersecurity including systems and personnel;
c. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;
d. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;
e. Ordering that Defendant's segment Plaintiff's and the Class's Private Information by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

f. Ordering that Defendant cease storing unencrypted Private Information on its systems;

g. Ordering that Defendant conduct regular database scanning and securing checks;

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

i. Ordering Defendant to implement and enforce adequate retention policies for Private Information, including destroying, in a reasonably secure manner, Private Information once it is no longer necessary for it to be retained; and

j. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

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

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Complaint.

Dated: September 12, 2022

Respectfully submitted,

_____

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (847) 208-4585
gklinger@milberg.com

William B. Federman
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
wbf@federmanlaw.com

A. Brooke Murphy
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
abm@murphylegalfirm.com

Attorneys for Plaintiff