UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN

KENNETH RATCLIFF, individually and on behalf of all others similarly situated, Plaintiff, v. MORLEY COMPANIES, INC., Defendant.	Case No. CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Kenneth Ratcliff ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through the undersigned attorneys, brings this Class Action Complaint against Defendant Morley Companies, Inc. ("Morley") and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Morley for its failure to secure and safeguard Plaintiff's and approximately 521,046 other individuals' ("Class members") private, confidential, and sensitive medical and personally identifying information ("PII/PHI"), including: names, addresses, Social Security numbers, dates of birth, client identification numbers, medical diagnostic and treatment information, and health insurance information.

2. Defendant is a company that provides various business services, such as customer service, meeting planning, and exhibit and display design.

3. On August 1, 2021, unauthorized individuals gained access to Morley's networks and accessed and copied the PII/PHI of Plaintiff and Class members (the "Data Breach").

4. Morley owed a duty to Plaintiff and Class members to implement and maintain

reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Morley breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its employees', former employees', and clients' PII/PHI from unauthorized access and disclosure.

5. As a result of Morley's inadequate security measures and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all other individuals whose PII/PHI was exposed as a result of the Data Breach.

6. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, negligence per se, breach of implied contract, unjust enrichment, and violation of the Michigan Consumer Protection Act, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

7. Plaintiff Kenneth Ratcliff is a Michigan resident who was previously employed by Morley. Believing Morley would implement and maintain reasonable security measures and practices to protect his PII/PHI, Plaintiff Ratcliff provided his PII/PHI to Morley, or Morley otherwise received his PII/PHI, in connection with obtaining employment from Morley. Plaintiff Ratcliff received a letter dated January 26, 2022 from Morley notifying him that his PII/PHI may have been exposed in the Data Breach. Had Plaintiff Ratcliff known that Morley does not adequately protect PII/PHI, he would not have agreed to provide Morley with his PII/PHI.

8. Defendant Morley Companies, Inc. is a Michigan corporation with its principal place of business located at One Morley Plaza, Saginaw, Michigan 46202.

JURISDICTION AND VENUE

9. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

10. This Court has personal jurisdiction over Morley because Morley is a corporation organized under the laws of Michigan.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Morley's principal place of business is located in Saginaw, Michigan.

FACTUAL ALLEGATIONS

Overview of Morley

12. Morley is an organization that provides three main services to businesses: business process outsourcing, meetings and incentives, and exhibits and displays.[1] The company's website states that it works with many Fortune 500 companies.[2]

13. In the regular course of its business, Morley collects and maintains the PII/PHI of employees, former employees, and its clients.

14. Morley requires employees to provide information before being hired and in order to participate in its health plan. That information includes, *inter alia*, names, addresses, dates of

[1] *Services*, MORLEY COMPANIES, INC., https://www.morleynet.com/Services/ (last accessed Feb. 10, 2022)
[2] *Id*.

birth, health insurance information, and Social Security numbers. Morley stores this information digitally.

15. Plaintiff and Class members are, or were, employees or clients of Morley or received services from Morley, and entrusted Morley with their PII/PHI.

The Data Breach

16. On or about August 1, 2021, an unauthorized individual, or unauthorized individuals, gained access to Morley's network systems.[3] Morley does not state when the unauthorized access concluded.

17. According to the Maine Attorney General, 521,046 individuals' PII/PHI was exposed during the breach.[4]

18. Morley did not begin to notify impacted breach victims about the data breach until six months after it learned of the breach in August 2021. The notice that Morley posted on its website on February 2, 2022 states the information that was accessed included:

> name, address, Social Security number, date of birth, client identification number, medical diagnostic and treatment information, and health insurance information.[5]

Morley Knew That Criminals Target PII/PHI

19. At all relevant times, Morley knew, or should have known that the PII/PHI was a target for malicious actors. Despite such knowledge, Morley failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that Morley should have anticipated and guarded against.

---

[3] *Morley Notifies Clients of Data Security Incident*, MORLEY COMPANIES, INC. (Feb. 2, 2022), available at https://www.morleynet.com/about/cyber-security-incident/ (last accessed Feb. 10, 2022).

[4] https://apps.web.maine.gov/online/aeviewer/ME/40/9779e52a-a15b-4cde-884e-7b25e4a56b80.shtml (last accessed Feb. 10, 2022)

[5] *Morley Notifies Clients of Data Security Incident*, n.3, *supra*.

20. It is well known amongst companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers ("SSNs") and medical information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[6]

21. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company Protenus found that there were 758 medical data breaches in 2020 with over 40 million patient records exposed.[7] This is an increase from the 572 medical data breaches that Protenus compiled in 2019.[8]

22. PII/PHI is a valuable property right.[9] The value of PII/PHI as a commodity is measurable.[10] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[11] American companies are estimated to have spent over $19 billion on acquiring

---

[6] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 AM), available at https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[7] Protenus, *2021 Breach Barometer*, PROTENUS.COM, available at https://www.protenus.com/resources/2021-breach-barometer (last accessed Feb. 10, 2022).

[8] Protenus, *2020 Breach Barometer*, PROTENUS.COM, available at https://www.protenus.com/resources/2020-breach-barometer (last accessed Feb. 10, 2022).

[9] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), available at https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data (last accessed Feb. 10, 2022).

[10] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), available at http://www.medscape.com/viewarticle/824192 (last accessed Feb. 10, 2022)..

[11] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (April 2, 2013), available at https://www.oecd-

personal data of consumers in 2018.[12] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

23. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

24. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[13] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[14] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[15]

25. All-inclusive health insurance dossiers containing sensitive health insurance

---

ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last accessed Feb. 10, 2022).

[12] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), available at https://www.iab.com/news/2018-state-of-data-report/ (last accessed Feb. 10, 2022).

[13] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), available at https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last accessed Feb. 10, 2022) ("*What Happens to Stolen Healthcare Data* Article") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[14] *Id.*

[15] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), available at https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims (last accessed Feb. 10, 2022).

information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[16] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[17]

26. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[18] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "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."[19]

27. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[20]

28. Given these facts, any company that transacts business with a consumer and then

---

16 SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), available at https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market (last accessed Feb. 10, 2021).

17 Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), available at https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last accessed Feb. 10, 2021).

18 *What Happens to Stolen Healthcare Data*, *supra* at n.13.

19 *Id.*

20 Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), available at https://www.jstor.org/stable/23015560?seq=1 (last accessed Feb. 10, 2021).

compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

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

29. Theft of PII/PHI is serious. The Federal Trade Commission ("FTC") warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[21]

30. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[22] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[23]

31. With access to an individual's PII/PHI, criminals can do more than just empty a

---

[21] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, available at https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Feb. 10, 2022).

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

[23] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, available at https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed Feb. 10, 2022).

victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits, or; filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[24]

32. Identity theft is a very difficult problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[25]

33. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

34. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[26]

---

[24] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV, available at https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Feb. 10, 2022).

[25] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), available at https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Feb. 10, 2022).

[26] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use*

35. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[27] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[28] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[29] The FTC also warns, "If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[30]

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

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

Social Security Numbers, Experts Say, TIME (August 5, 2019), available at https://time.com/5643643/capital-one-equifax-data-breach-social-security/ (last accessed Feb. 10, 2022).

[27] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), available at https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf

[28] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* at n.17.

[29] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, available at https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Feb. 10, 2022).

[30] *Id*.

victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[31]

37. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average, it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[32]

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

Damages Sustained by Plaintiff and the Other Class Members

39. Plaintiff and Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and

[31] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* at 27.
[32] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), available at http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf (last accessed Feb. 10, 2021).

international market; and (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

CLASS ALLEGATIONS

40. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23.

41. Plaintiff brings this action on behalf of himself and all members of the following Class of similarly situated persons:

> All individuals whose PHI/PII was accessed by and disclosed to unauthorized persons in the Data Breach, including all individuals who were sent a notice of the Data Breach.

42. Excluded from the Class is Morley Companies, Inc. and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

43. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

44. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. Morley reported to the Maine Attorney General that approximately 521,046 individuals' information was exposed in the Data Breach.

45. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Morley had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;

b. Whether Morley failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

c. Whether an implied contract existed between Class members and Morley providing that Morley would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

d. Whether Morley breached its duties to protect Plaintiff's and Class member's PII/PHI; and

e. Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

46. Morley engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

47. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Morley, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

48. Plaintiff will fairly and adequately protect the interests of the Class members.

Plaintiff is an adequate representative of the Class in that Plaintiff has no interests adverse to, or that conflict with, the Class he seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

49. 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. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Morley, so it would be impracticable for Class members to individually seek redress from Morley's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a 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 single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

50. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

51. Morley owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

52. Morley knew the risks of collecting and storing Plaintiff's and Class members'

PII/PHI and the importance of maintaining secure systems. Morley knew of the many data breaches that targeted businesses that collect sensitive PII/PHI in recent years.

53. Given the nature of Morley's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Morley should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

54. Morley breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

55. It was reasonably foreseeable to Morley that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

56. But for Morley's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

57. As a result of Morley's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to

compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT II

NEGLIGENCE PER SE

58. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

59. Morley's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Morley, of failing to employ reasonable measures to protect and secure PII/PHI.

60. Morley violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and Class members' PII/PHI and not complying with applicable industry standards. Morley's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

61. Morley's violation of Section 5 of the FTCA constitutes negligence per se.

62. Plaintiff and Class members are within the class of persons that Section 5 of the FTCA was intended to protect.

63. The harm occurring as a result of the Data Breach is the type of harm Section 5 of

the FTCA weas 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 practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and Class members as a result of the Data Brach.

64. It was reasonably foreseeable to Morley that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

65. The injury and harm that Plaintiff and Class members suffered was the direct and proximate result of Morley's violations of Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT III

BREACH OF IMPLIED CONTRACT

66. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully

set forth herein.

67. In connection with receiving employment or business services, Plaintiff and Class members entered into implied contracts with Morley.

68. Pursuant to these implied contracts, Plaintiff and Class members provided Morley with their PII/PHI. In exchange, Morley agreed to, among other things, and Plaintiff understood that Morley would: (1) provide employment or other business services to Plaintiff and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) protect Plaintiff's and Class members' PII/PHI in compliance with federal and state laws and regulations and industry standards.

69. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Morley, on the other hand. Had Plaintiff and Class members known that Morley would not adequately protect its employees' and clients' PII/PHI, they would not have received medical treatment or services from Morley.

70. Plaintiff and Class members performed their obligations under the implied contract when they provided Morley with their PII/PHI, worked for Morley, and paid for services from Morley.

71. Morley breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

72. Morley's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and Class members

have suffered from the Data Breach.

73. Plaintiff and Class members were damaged by Morley's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT IV

UNJUST ENRICHMENT

74. Plaintiff realleges and incorporate by reference all preceding paragraphs as if fully set forth herein.

75. This claim is pleaded in the alternative to the breach of implied contract claim.

76. Plaintiff and Class members conferred a monetary benefit upon Morley in the form of working for Morley or monies paid for business services.

77. Morley accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members. Morley also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate payment or provide business services.

78. As a result of Morley's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between what Plaintiff and Class members were paid for their employment or their payments made with reasonable data privacy and security

practices and procedures that Plaintiff and Class members worked for or paid for, and those payments to or from Morley without reasonable data privacy and security practices and procedures that they received.

79. Morley should not be permitted to retain the money belonging to Plaintiff and Class members because Morley failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

80. Morley should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V

VIOLATIONS OF THE MICHIGAN CONSUMER PROTECTION ACT
Mich. Comp. Laws §§ 445.901 *et seq*. ("MCPA")

81. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

82. Plaintiff and Defendant are "persons" under the MCPA. Mich. Comp. Laws § 445.902(d).

83. Defendant's transactions and conducting of business, namely providing employment, business process outsourcing, meetings and incentives, and exhibits and displays, with Plaintiff and Michigan Class members is "trade or commerce" under the MCPA. Mich. Comp. Laws § 445.902(g).

84. The MCPA lists 38 categories of practices that are considered unfair, unconscionable, or deceptive, and thus unlawful, under the statute. Mich. Comp. Laws § 445.903. Defendant's conduct in providing employment, business process outsourcing, meetings and

incentives, and exhibits and displays to Plaintiff and Class members while omitting or concealing that its data privacy practices are inadequate and that the sensitive information entrusted to it was exposed to a breach, constitutes unfair, unconscionable, deceptive, and thus unlawful, practices in at least the following categories:

a. "Representing that . . . services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have . . ." Mich. Comp. Laws § 445.903(c);

b. "Representing that . . . services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another" Mich. Comp. Laws § 445.903(e);

c. "Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer" Mich. Comp. Laws § 445.903(s); and

d. "Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner" Mich. Comp. Laws § 445.903(cc).

85. Had Plaintiff and Class members been aware of the omitted and misrepresented facts, i.e., that Morley does not value data privacy and does not protect sensitive information, Plaintiff and the other Class members would not have sought employment or other services from Morley.

86. Pursuant to Mich. Comp. Laws § 445.911(4), Plaintiff Ratcliff seeks damages on behalf of himself and all Class members.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in his favor and against Morley as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of themselves and the Class, seeks appropriate injunctive relief designed to prevent Morley from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: February 18, 2022

Respectfully submitted,

/s/ *Nicholas A. Coulson*
NICHOLAS A. COULSON (P78001)

ncoulson@lsccounsel.com
LANCE SPITZIG (P84988)
lspitzig@lsccounsel.com
LIDDLE SHEETS COULSON P.C.
975 E. Jefferson Avenue
Detroit, MI 48207
Tel: 313.392.0015
Fax: 313.392.0025

BEN BARNOW*
b.barnow@barnowlaw.com
ANTHONY L. PARKHILL*
aparkhill@barnowlaw.com
RILEY W. PRINCE*
rprince@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504

ANDREW W. FERICH*
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

TINA WOLFSON*
twolfson@ahdootwolfson.com
ROBERT AHDOOT*
rahdoot@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

**pro hac vice* to be submitted