UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO

MICHAEL DOYLE, on behalf of himself and others similarly situated,	:	
Plaintiff,	:	**Civil Action No. 1:20-cv-908**
v.	:	**CLASS ACTION COMPLAINT**
LUXOTTICA OF AMERICA, INC.,	:	**JURY TRIAL DEMANDED**
Defendant.	:	

1. Michael Doyle ("Plaintiff"), individually, and on behalf of others similarly situated, brings this action against Luxottica of America, Inc. ("Luxottica" or "Defendant") to obtain damages, restitution, and injunctive relief for the class and subclass, as defined below, from Defendant.

2. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

Nature of the Action

3. This class action arises out of a recent cyberattack and data breach ("Data Breach") involving Luxottica's network of eyecare facilities.

4. Through this Data Breach, an "unauthorized actor gained access to [Defendant's] scheduling application," and through this access, "the attacker may have accessed and acquired patient information."[1]

[1] *See* Exhibit A.

5. As a result of the Data Breach, Plaintiff and countless other members of the proposed class suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

6. In addition, Plaintiff's sensitive personal information—which was entrusted to Defendant, its officials and agents—was compromised and unlawfully accessed due to the Data Breach.

7. Information compromised in the Data Breach includes names, demographic information, dates of birth, Social Security numbers, health insurance information, medical information, other protected health information as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), and additional personally identifiable information ("PII") and protected health information ("PHI") that Defendant collected and maintained (collectively, the "Private Information").

8. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of class members' Private Information that it collected and maintained, and for failing to provide sufficient notice to Plaintiff and other class members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

9. Defendant maintained the Private Information in a reckless manner because the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks.

10. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and class members' Private Information was a known risk to

Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a vulnerable condition.

11. In addition, Defendant and its employees or agents failed to properly monitor the computer network and systems that housed the Private Information.

12. Had Defendant properly monitored its property, it would have discovered the intrusion sooner.

13. Plaintiff's and class members' identities are now at risk because of Defendant's negligent conduct because the Private Information that Defendant collected and maintained is now in the hands of data thieves.

14. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, but not limited to, opening new financial accounts in class members' names, taking out loans in class members' names, using class members' names to obtain medical services, using class members' health information to target other phishing and hacking intrusions based on their individual health needs, using class members' information to obtain government benefits, filing fraudulent tax returns using class members' information, obtaining driver's licenses in class members' names but with another person's photograph, and giving false information to police during an arrest.

15. As a result of the Data Breach, Plaintiff has been exposed to a heightened and imminent risk of fraud and identity theft, and Plaintiff must now and in the future closely monitor his financial and vision insurance accounts to guard against identity theft.

16. Plaintiff may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

17. By way of this action, Plaintiff seeks to remedy these harms on behalf of himself and similarly situated individuals whose Private Information was accessed during the Data Breach.

18. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

19. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) intrusion upon seclusion, (iii) negligence *per se*, (iv) breach of express contract, (v) breach of implied contract, (vi) breach of fiduciary duty, (vii) violations of the Fair Credit Reporting Act, and, (viii) violation of the Connecticut Unfair Trade Practices Act.

Parties

20. Mr. Doyle is a natural person who at all relevant times resided in New London County, Connecticut.

21. Defendant is an international eyewear conglomerate with its American subsidiary and retail division headquartered in Mason, Ohio.

22. Defendant designs, sells, and licenses various brands of eyewear, operates numerous retail and optometry chains, and also operates one of the largest vision benefits insurance companies in the United States.

Jurisdiction and Venue

23. This Court has federal question subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because the Plaintiff asserts claims that necessarily raise substantial disputed federal issues under HIPAA, the Federal Trade Commission Act (15 U.S.C. § 45), the Gramm-

Leach-Bliley Act (15 U.S.C. § 6801), and the Fair Credit Reporting Act ("FCRA") (15 U.S.C. § 1681 *et seq.*).

24. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events and omissions giving rise to these claims occurred in this district, and because Defendant is headquartered in this district.

Defendant's Business

25. Defendant is a U.S. subsidiary of Luxottica Group S.p.A., an Italian eyewear conglomerate.

26. Defendant produces and licenses eyewear under numerous brand names, including Ray-Ban, Oakley, Chanel, and Polo Ralph Lauren, among many others.[2]

27. Defendant operates numerous eyewear retail locations, including brands such as Sunglass Hut, LensCrafters, Pearle Vision, and Ray-Ban, among many others.[3]

28. Defendant also operates EyeMed Vision Care, "the second largest vision benefits company in the United States, serving approximately 52 million members in large, medium and small-sized companies, as well as government entities."[4]

29. As part of some of its retail operations, Defendant provides optometry and vision services to consumers.

---

[2] http://www.luxottica.com/en/eyewear-brands (last visited November 9, 2020).

[3] http://www.luxottica.com/en/retail-brands (last visited November 9, 2020).

[4] http://www.luxottica.com/en/retail-brands/eyemed-vision-care (last visited November 9, 2020).

30. As a result, in the ordinary course of receiving treatment and health care services from Defendant, patients are required to provide Defendant with sensitive, personal and private information such as:

- Name, address, telephone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Information relating to individual medical history;
- Insurance information and coverage;
- Information concerning an individual's doctor, nurse or other medical providers;
- Photo identification;
- Employer information, and;
- Other information that may be deemed necessary to provide care or facilitate billing.

31. Defendant also gathers certain medical information about patients and creates records of the care it provides to them.

32. Additionally, Defendant may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care", such as referring optometrists, patients' other doctors, patients' health plan(s), close friends, and/or family members.

33. Defendant's healthcare employees, staff, and related entities may share patient information with each other for various purposes without a written authorization, as disclosed in its Notice of Privacy Practices (the "Privacy Notice"):[5]

> For Treatment. We may use or disclose your health information to an optometrist, ophthalmologist, optician or other health care providers providing treatment to you for:
> the provision, coordination, or management of health care and related services by health care providers;
> consultation between health care providers relating to a patient/customer;
> the referral of a patient for health care from one health care provider to another; or
> appointment and refill reminders, and recall information.
>
> For Payment. We may use and disclose your health information to others for purposes of processing and receiving payment for treatment and services provided to you. This may include:
> billing and collection activities and related data processing;
> actions by a health plan or insurer to determine or fulfill its responsibilities for coverage and provision of benefits under its health plan or insurance agreement, determinations of eligibility or coverage, adjudication or subrogation of health benefit claims;
> medical necessity and appropriateness of care reviews, utilization review activities; and
> disclosure to consumer reporting agencies of information relating to collection of payments.
>
> For Health Care Operations. We may use and disclose health information about you for health care operational purposes. For example, your health information may be disclosed to:
> evaluate the performance of our associates;
> assess the quality of service, product and care in your case and similar cases;
> learn how to improve our facilities and services;
> conduct training programs or credentialing activities;
> facilitate compliance functions, auditing and legal services;
> determine how to continually improve the quality and effectiveness of the products, service and care we provide, including customer satisfaction surveys and data analyses;
> properly manage our business, including acquisitions, mergers and consolidations; and
> communicate with you concerning (a) a health-related product or service that is provided by us, (b) your treatment, or (c) case management, care coordination or to

[5] *See, e.g.*, https://www.pearlevision.com/m20ContentView?catalogId=15951&langId=-1&storeId=12002&page=legal#PrivacyPractices (last visited November 9, 2020); *infra* n.7.

> recommend alternative treatments, therapies, providers or settings for care to the extent such activities are not within your current treatment. However, if we receive compensation for making a communication concerning another entity's products or services (other than payment for treatment), the communication is "marketing" and will require that we obtain your prior written authorization as described in the Marketing section, below.

34. The current privacy notice has an effective date of January 13, 2011.

35. The Privacy Notice is posted on Defendant's website.

36. Because of the potentially highly sensitive and personal nature of the information Defendant acquires and stores with respect to its patients, Defendant promises to, among other things, : A) to "Maintain the privacy and safeguard the security of your health information;" B) to inform and notify patients "when you, along with all other affected individuals, of a breach of unsecured health information;" and C) "Unless you give us a written authorization, we cannot use or disclose your health information for any reason except those described in this Notice."[6]

37. Defendant also publishes a standardized privacy statement for its various entities consistent with these practices, titled "LUXOTTICA OF AMERICA INC. NOTICE OF PRIVACY PRACTICES."[7]

The Cyberattack and Data Breach

38. On or about August 5, 2020, Defendant suffered the Data Breach on its "web-based appointment scheduling platform that is used by its patients to schedule appointments online or over the phone."[8]

---

6 *Id.*

7 https://s7d9.scene7.com/is/content/Lenscrafters/PrivacyPolicy/NPP_Final_Version_2.28.2019.pdf (last visited November 9, 2020).

8 https://securityaffairs.co/wordpress/110565/data-breach/luxottica-lenscrafters-eyemed-data-breach.html (last visited November 9, 2020).

39. According to a "Security Incident" notification issued by Defendant on or about October 28, 2020, it first became aware of the hack on August 9, 2020, and, after investigating the attack, determined on August 28, 2020 that the hackers gained access to patients' personal information.[9]

40. Through the notice, Defendant "confirm[ed] the exposure of information including personal data (PII) and protected health information (PHI), such as medical conditions and history. For some patients, exposed information included credit card numbers and social security numbers."[10]

41. Despite the fact that Defendant warrants to consumers in its Privacy Notice that, "if we discover that your health information has been breached . . . and the privacy or security of the information has been compromised, we must notify you of the breach without unreasonable delay and in no event later than 60 days following our discovery of the breach," Defendant first became aware of the hack on August 9, 2020 and, after investigating the attack, determined on August 28, 2020 that the threat actors gained access to patients' personal information.

42. The Data Breach originated from Defendant's appointment scheduling platform, though the method of the Data Breach still has not been disclosed.

---

9 *See* https://luxottica.kroll.com/ (last visited November 9, 2020); Ex. A.

10 *Supra* n.8.

43. Though Defendant has not disclosed the total number of affected consumers, Defendant's EyeMed insurance platform has over 52,000,000 subscribers,[11] LensCrafters has over 900 retail locations,[12] and Pearle Vision has over 500 retail locations.[13]

44. Plaintiff believes his Private Information was stolen (and, potentially, subsequently sold) in the Data Breach.

45. On or about October 28, 2020, Plaintiff received a letter from Defendant informing him that his Private Information was "accessed and acquired" by an unauthorized actor, and that "the personal information involved in this incident may have included your full name, contact information, appointment date and time, and health insurance policy number."[14]

46. Prior to receiving this letter, on or about July 2020, Plaintiff visited a Pearle Vision optometrist in Waterford, Connecticut, obtained an annual vision exam, and purchased new prescription glasses.

47. As part of this process, Plaintiff provided his social security number, vision insurance information, and relevant medical history to Defendant or Defendant's employees.

48. While Defendant claimed it was "not aware of any misuse of personal information or harm to patients as a result of this incident," it could not rule out the possibility.[15]

---

[11] *See* Luxottica 2018 Annual report, available at http://www.luxottica.com/sites/luxottica.com/files/luxottica_group_relazione_finanziaria_annuale_2018_eng_20190410.pdf (last visited November 10, 2020).

[12] https://local.lenscrafters.com/#:~:text=918%20LensCrafters%20Stores%20in%20the%20United%20States&text=Map%20of%20the%20United%20States%20with%20states%20in%20which%20we%20operate%20highlighted (last visited November 10, 2020).

[13] http://www.luxottica.com/en/retail-brands/pearle-vision (last visited November 10, 2020).

[14] Ex. A.

[15] *Id.*

49. Further, this consumer data breach coincides with a ransomware cyberattack in September 2020 involving Defendant's parent company, in which "some of the web sites operated by [Defendant] were not reachable, including Ray-Ban, Sunglass Hut, LensCrafters, EyeMed, and Pearle Vision."[16]

50. Thereafter, a "huge trove of files" was posted on the dark web, "related to the personnel office and finance departments."[17]

51. Cybersecurity intelligence firm Bad Packets postulated that the cause of the ransomware attack was "a Citrix ADX controller device vulnerable to the critical CVE-2019-19781 flaw."[18]

52. As a result, Defendant, and Defendant's international parent company, have seemingly suffered two serious data breaches in as many months, indicating systemic problems in Defendant's cybersecurity practices.

53. Defendant had obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiff and the class members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

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

---

16 https://securityaffairs.co/wordpress/108611/cyber-crime/luxottica-cyber-attack.html (last visited November 9, 2020).

17 https://securityaffairs.co/wordpress/109778/data-breach/luxottica-data-leak-ransomware.html (last visited November 9, 2020); *see also* https://www.itwire.com/security/eyewear-giant-luxottica-hit-by-windows-nefilim-ransomware,-data-leaked.html (last visited November 9, 2020).

18 https://www.bleepingcomputer.com/news/security/ray-ban-owner-luxottica-confirms-ransomware-attack-work-disrupted/ (last visited November 9, 2020).

55. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks or data breaches in the healthcare industry preceding the date of the breach.

56. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

57. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[19]

58. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

59. Defendant breached its obligations to Plaintiff and the class members or was otherwise negligent and reckless because it failed to properly maintain and safeguard Defendant's computer systems and data.

60. Defendant's unlawful conduct includes, but is not limited to, the following acts or omissions:

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

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

[19] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last visited November 9, 2020).

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

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

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

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

k. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); or

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. 45 C.F.R. § 164.304.

61. As the result of computer systems in dire need of security upgrading and inadequate procedures for handling unauthorized user access to appointment data, Defendant negligently and unlawfully failed to safeguard Plaintiff's and class members' Private Information.

62. Accordingly, as outlined below, Plaintiff's and class members' daily lives were severely disrupted.

63. As a result, Plaintiff and the class members now face an increased risk of fraud and identity theft.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identify Theft

64. Cyberattacks and data breaches involving medical practices like Defendant's are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

65. Indeed, researchers have found that, at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.[20]

66. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[21]

67. Similarly, cyberattacks and related data security incidents inconvenience patients. The various inconveniences patients encounter as a result of such incidents include, but are not limited to:

a. rescheduling medical treatment;

b. finding alternative medical care and treatment;

c. delaying or foregoing medical care and treatment;

---

[20] *See* https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last visited November 8, 2020).

[21] *See* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited November 8, 2020)/

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

e. losing patient medical history.[22]

68. Cyberattacks are considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> *Breach* means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the [PHI].[23]

69. Data breaches represent yet another problem for patients who have already experienced inconvenience and disruption associated with a cyberattack.

70. The United States Government Accountability Office released a data breach report in 2007 in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[24]

71. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (instructing to consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove

---

[22] *See, e.g.*, https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/ (last visited November 8, 2020); https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech (last visited November 8, 2020).

[23] 45 C.F.R. § 164.402; *see also* 45 C.F.R. 164.40 ("The requirements of this subpart shall apply with respect to breaches of protected health information occurring on or after September 23, 2009.).

[24] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited November 8, 2020) ("GAO Report").

fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[25]

72. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

73. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, 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. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[26]

[25] *See* https://www.identitytheft.gov/Steps (last visited November 8, 2020).

[26] https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141445.pdf (last visited June 20, 2019). (last visited November 8, 2020).

Figure 35: How has your life been impacted by this crime (Check all that apply)						
	2015	2014	2013	2009	2008	2007
My ability to get credit cards was affected and or I was denied a credit card	31.8%	32.7%	32.4%	53.0%	45.0%	52.0%
Ability to obtain other types of loans was affected and/or I was denied other types of loans	28.0%	28.4%	32.4%	40.0%		
Ability to obtain other financial accounts (such as checking or savings) was affected and/or I was unable to open other financial accounts	18.0%	16.7%	22.9%	this answer was not provided		
Interest rates on existing credit cards increased	11.3%	14.4%	12.9%	21.0%	33.0%	36.0%
Credit card/s I had was cancelled	14.6%	16.3%	13.9%	29.0%	34.0%	27.0%
Collection agencies still calling	21.3%	19.5%	22.3%	47.0%	39.0%	53.0%
My ability to get a job has been affected and/or I have been unable to get a job	15.5%	12.1%	14.5%	14.0%	23.0%	18.0%
Lost my job	9.6%	3.5%	5.0%	3.0%	5.0%	N/A
Unable to pay bills	17.6%	15.2%	17.9%	23.0%	28.0%	N/A
None of these apply	38.9%	39.7%	27.3%	this answer was not provided		
Other	24.3%	22%	25.7%	this answer was not provided		

74. What's more, theft of Private Information is also gravely serious since PII/PHI is a valuable property right.[27]

75. The value of Private Information is axiomatic, considering the value of various tech companies transacting primarily in the sale of personal data, and the consequences of cyber thefts often include heavy prison sentences.

[27] *See, e.g.*, John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at 3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

76. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[28]

77. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at p. 29.

78. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

79. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and the class members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and the class members must vigilantly monitor their financial and medical accounts for many years to come.

[28] *See* http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited last visited November 8, 2020).

80. Medical information is especially valuable to identity thieves: "According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $50 and up."[29]

81. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

82. As a result, Defendant knew or should have known of this heightened risk of data theft and strengthened its data systems accordingly.

83. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

Plaintiff's and Class Members' Damages

84. To date, Defendant has done absolutely nothing to provide Plaintiff and the class members with relief for the damages they have suffered as a result of the Data Breach.

85. Plaintiff and the class members have been damaged by the compromise of their Private Information in the Data Breach.

86. Plaintiff's Private Information was stolen and is now in the hands of data thieves as a direct and proximate result of the Data Breach.

87. As a direct and proximate result of Defendant's conduct, Plaintiff and the class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

[29] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited last visited November 8, 2020).

88. As a direct and proximate result of Defendant's conduct, Plaintiff and the class members have been forced to expend time dealing with the effects of the Data Breach.

89. Plaintiff and the class members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

90. Plaintiff and the class members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and the class members.

91. Plaintiff and the class members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

92. Plaintiff and the class members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach.

93. As a result of the Data Breach, Plaintiff and the class members overpaid for Defendant's service that was intended to be accompanied by adequate data security, but was not.

94. Part of the price Plaintiff and the class members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer property and Plaintiff's and class members' Private Information, and Plaintiff and the class members did not get what they bargained for.

95. Plaintiff and the class members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

96. Plaintiff and the class members have suffered or will suffer actual injury as a direct result of the Data Breach.

97. Specifically, Data Breach victims suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts, medical accounts, and credit reports for unauthorized activity for years to come.

98. Moreover, Plaintiff and the class members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

99. Further, as a result of Defendant' conduct, Plaintiff and the class members are forced to live with the anxiety that their Private Information—which can contain the most intimate details about a person's life, including their medical history—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

100. As a direct and proximate result of Defendant' actions and inactions, Plaintiff and the class members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

Class Action Allegations

101. Plaintiff brings this action under Federal Rule of Civil Procedure 23, and as a representative of the following class and subclass:

> National Class: All persons who used Luxottica of America, Inc.'s appointment booking services and whose Private Information was maintained on Luxottica of America, Inc.'s system that was compromised in the Data Breach.
>
> Connecticut Subclass: All residents of Connecticut who used Luxottica of America, Inc.'s appointment booking services and whose Private Information was maintained on Luxottica of America, Inc.'s system that was compromised in the Data Breach.

Excluded from the class and subclass are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant.

102. Also excluded also from the class and subclass are members of the judiciary to whom this case is assigned, their families and members of their staff.

103. Plaintiff's claims, and the claims of the members of the class and subclass, originate from the same conduct, practice, and procedure on the part of Defendant.

104. Plaintiff's claims are based on the same theories as the claims of the members of the class and subclass.

105. Plaintiff suffered the same injuries as the members of the class and subclass.

106. Plaintiff will fairly and adequately protect the interests of the members of the class and subclass.

107. Plaintiff's interests in this matter are not directly or irrevocably antagonistic to the interests of the members of the class and subclass.

108. Plaintiff will vigorously pursue the claims of the members of the class and subclass.

109. Plaintiff has retained counsel experienced and competent in class action litigation.

110. Plaintiff's counsel will vigorously pursue this matter.

111. Plaintiff's counsel will assert, protect, and otherwise represent the members of the class and subclass.

112. The questions of law and fact common to the members of the class and subclass predominate over questions that may affect individual members of the class and subclass.

113. Issues of law and fact common to all members of the class and subclass are:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and class members' Private Information;

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

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, HIPAA;

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

e. Whether Defendant owed a duty to class members to safeguard their Private Information;

f. Whether Defendant breached its duty to the class members to safeguard their Private Information;

g. Whether computer hackers obtained class members' Private Information in the Data Breach;

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

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

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was *per se* negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

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

n. Whether Plaintiff and the class members are entitled to damages, treble damages, civil penalties, punitive damages, or injunctive relief.

114. A class action is superior to all other available methods for the fair and efficient adjudication of this matter.

115. If brought and prosecuted individually, the claims of the members of the class and subclass would require proof of the same material and substantive facts.

116. The pursuit of separate actions by individual members of the class and subclass would, as a practical matter, be dispositive of the interests of other members of the class and subclass, and could substantially impair or impede their ability to protect their interests.

117. The pursuit of separate actions by individual members of the class and subclass could create a risk of inconsistent or varying adjudications, which might establish incompatible standards of conduct for Defendant.

118. These varying adjudications and incompatible standards of conduct, in connection with presentation of the same essential facts, proof, and legal theories, could also create and allow the existence of inconsistent and incompatible rights within the class and subclass.

119. The damages suffered by individual members of the class and subclass may be relatively small, thus, the expense and burden to litigate each of their claims individually make it difficult for the members of the class and subclass to redress the wrongs done to them.

120. The pursuit of Plaintiff's claims, and the claims of the members of the class and subclass, in one forum will achieve efficiency and promote judicial economy.

121. There will be little difficulty in the management of this action as a class action.

122. Defendant has acted or refused to act on grounds generally applicable to the members of the class and subclass, making final declaratory or injunctive relief appropriate.

Causes of Action

First Count
Negligence
(On Behalf of Plaintiff and National Class members)

123. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-122.

124. Defendant required Plaintiff and National Class members to submit non-public personal information in order to obtain medical services.

125. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and National Class members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft.

126. Defendant's duty also included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

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

128. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its client patients, such as Plaintiff, which is recognized by laws and regulations including but not limited to HIPAA, as well as

common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to National Class members from a data breach.

129. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

130. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

131. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

132. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

133. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and National Class members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard class members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their appointment booking system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to class members' Private Information;

e. Failing to detect in a timely manner that class members' Private Information had been compromised; and

f. Failing to timely notify Plaintiff and class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

134. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and National Class members' Private Information would result in injury to National Class members.

135. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

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

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

138. Plaintiff and National Class members are also entitled to injunctive relief requiring Defendant to, among other things, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to Plaintiff and all National Class members.

Second Count

Intrusion Upon Solitude / Invasion of Privacy
(On Behalf of Plaintiff and National Class members)

139. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-122.

140. The States of Ohio[30] and Connecticut[31] recognize the tort of invasion of privacy, break it down into four categories including intrusion upon solitude (seclusion), and adopt the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

141. Plaintiff and National Class members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

142. Defendant's conduct as alleged above intruded upon Plaintiff's and National Class members' seclusion under common law.

143. By intentionally failing to keep Plaintiff's and National Class members' Private Information safe, and by intentionally misusing or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff's and National Class members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and National Class members' private affairs in a manner that identifies Plaintiff and National Class

---

30 *See, e.g., Hidey v. Ohio State Highway Patrol*, 116 Ohio App. 3d 744, 749 (1996).

31 *See, e.g., Neron v. Cossette*, No. CV116003350S, 2012 WL 1592174, at *3 (Conn. Super. Ct. Apr. 13, 2012).

members and that would be highly offensive and objectionable to an ordinary person; and

b. Intentionally publicizing private facts about Plaintiff and National Class members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and National Class members.

144. Defendant knew that an ordinary person in Plaintiff's or National Class members' position would consider Defendant's intentional actions highly offensive and objectionable.

145. Defendant invaded Plaintiff's and National Class members' right to privacy and intruded into Plaintiff's and National Class members' private affairs by intentionally misusing or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

146. Defendant intentionally concealed from Plaintiff and National Class members an incident that misused or disclosed their Private information without their informed, voluntary, affirmative, and clear consent.

147. The conduct described above was directed at Plaintiff and the National Class members.

148. As a proximate result of such intentional misuse and disclosures, Plaintiff's and National Class members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted.

149. Defendant's conduct amounted to a substantial and serious invasion of Plaintiff's and National Class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

150. In failing to protect Plaintiff's and National Class members' Private Information, and in intentionally misusing or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and National Class members' rights to have such information kept confidential and private.

151. Plaintiff, therefore, seeks an award of damages on behalf of himself and the Nationwide Class.

Third Count

Breach of Express Contract
(On Behalf of Plaintiff and National Class members)

152. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-122.

153. Plaintiff and National Class members entered into valid and enforceable express contracts, or were third party beneficiaries of valid and enforceable express contracts, with Defendant.

154. The valid and enforceable express contracts that Plaintiff and National Class members entered into with Defendant include Defendant's promise to protect from disclosure nonpublic personal information given to Defendant or that Defendant gathers on its own.

155. Under these express contracts, Defendant or its affiliated vision healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and National Class members; and (b) protect Plaintiff's and the National Class members' PII/PHI: (i) provided to obtain such healthcare; or (ii) created as a result of providing such healthcare.

156. In exchange for these promises, Plaintiff and National Class members agreed to pay money for these services. In fact, Plaintiff paid more than $100 to Defendant for goods and services in July 2020.

157. Both the provision of healthcare and the protection of Plaintiff's and National Class members' PII/PHI were material aspects of these contracts.

158. At all relevant times, Defendant expressly represented in its Privacy Policy that it was required by law, *e.g.*,: A) to "Maintain the privacy and safeguard the security of your health information;" B) to inform and notify patients "when you, along with all other affected individuals, of a breach of unsecured health information;" and C) "Unless you give us a written authorization, we cannot use or disclose your health information for any reason except those described in this Notice."[32]

159. Defendant further expressly represented in its Privacy Policy document that its patients, including Plaintiff and National Class members, have a right to privacy of medical records and personal information.

160. Defendant's express representations, including, but not limited to, express representations found in its Privacy Policy, formed an express contract requiring Defendant's to implement data security adequate to safeguard and protect the privacy of Plaintiff's and National Class members' PII/PHI.

161. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their PII/PHI associated with obtaining healthcare private; so, to customers such as Plaintiff and National Class members, healthcare that does not adhere to industry standard data security protocols to protect PII/PHI is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

[32] https://www.lenscrafters.com/lc-us/hipaa (last visited November 9, 2020).

162. Plaintiff and National Class members would not have entered into these contracts with Defendant or its affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their PII/PHI would be safeguarded and protected.

163. A meeting of the minds occurred, as Plaintiff and members of the Nationwide Class provided their PII/PHI to Defendant or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, protection of their PII/PHI.

164. Plaintiff and National Class members performed their obligations under the contract when they paid for their health care services.

165. Defendant materially breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

166. Defendant materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices.

167. Specifically, Defendant did not comply with industry standards, or otherwise protect Plaintiff's and the National Class members' PII/PHI, as set forth above.

168. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

169. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and National Class members did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts.

170. Plaintiff and National Class members were accordingly damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

171. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither Plaintiff, National Class members, nor any reasonable person would have purchased healthcare from Defendant or its affiliated healthcare providers.

172. As a direct and proximate result of the Data Breach, Plaintiff and National Class members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their PII/PHI, the loss of control of their PII/PHI, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, emotional distress, anxiety, loss of privacy, and the loss of the benefit of the bargain they had struck with Defendant.

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

Fourth Count

Breach of Implied Contract
(On Behalf of Plaintiff and National Class members)

174. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-122.

175. When Plaintiff and National Class members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

176. Defendant solicited and invited Plaintiff and National Class members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and National Class members accepted Defendant's offers and provided their Private Information to Defendant.

177. In entering into such implied contracts, Plaintiff and National Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

178. Plaintiff and National Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

179. Plaintiff and National Class members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

180. Plaintiff and National Class members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

181. Plaintiff and National Class members fully and adequately performed their obligations under the implied contracts with Defendant.

182. Defendant breached its implied contracts with Plaintiff and National Class members by failing to safeguard and protect their Private Information.

183. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and National Class members sustained damages as alleged herein.

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

185. Plaintiff and National Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all National Class members.

Fifth Count

Negligence *Per Se*
(On Behalf of Plaintiff and National Class members)

186. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-122.

187. Pursuant to the Federal Trade Commission Act, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and National Class members' Private Information. 15 U.S.C. § 45.

188. Pursuant to HIPAA, Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and National Class members' Private Information. 42 U.S.C. § 1302d, *et seq.*

189. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." 45 C.F.R. § 164.304.

190. Pursuant to the Gramm-Leach-Bliley Act, Defendant had a duty to protect the security and confidentiality of Plaintiff's and National Class members' Private Information. 15 U.S.C. § 6801.

191. Pursuant to the FCRA, Defendant had a duty to adopt, implement, and maintain adequate procedures to protect the security and confidentiality of Plaintiff's and National Class members' Private Information. 15 U.S.C. § 1681(b).

192. Defendant breached its duties to Plaintiff and National Class members under the Federal Trade Commission Act, HIPAA, the FCRA, and the Gramm-Leach-Bliley Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and National Class members' Private Information.

193. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

194. But-for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and National Class members, Plaintiff and National Class members would not have been injured.

195. The injury and harm suffered by Plaintiff and National Class members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and National Class members to experience the foreseeable harms associated with the exposure of their Private Information.

196. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and National Class members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

Sixth Count

Breach of Fiduciary Duty
(On Behalf of Plaintiff and National Class members)

197. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-122.

198. In light of the special relationship between Defendant and Plaintiff and National Class members, whereby Defendant became guardians of Plaintiff's and National Class members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiff and National Class members, (1) for the safeguarding of Plaintiff's and National Class members' Private Information; (2) to timely notify Plaintiff and National Class members of a data breach and disclosure; and (3) maintain complete and accurate records of what patient information (and where) Defendant did and does store.

199. Defendant has a fiduciary duty to act for the benefit of Plaintiff and National Class members upon matters within the scope of its patients' relationship, in particular, to keep secure the Private Information of its patients.

200. Defendant breached its fiduciary duties to Plaintiff and National Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

201. Defendant breached its fiduciary duties to Plaintiff and National Class members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and National Class members' Private Information.

202. Defendant breached its fiduciary duties owed to Plaintiff and National Class members by failing to timely notify or warn Plaintiff and National Class members of the Data Breach.

203. Defendant breached its fiduciary duties owed to Plaintiff and National Class members by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

204. Defendant breached its fiduciary duties owed to Plaintiff and National Class members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

205. Defendant breached its fiduciary duties owed to Plaintiff and National Class members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

206. Defendant breached its fiduciary duties owed to Plaintiff and National Class members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

207. Defendant breached its fiduciary duties owed to Plaintiff and National Class members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

208. Defendant breached its fiduciary duties owed to Plaintiff and National Class members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

209. Defendant breached its fiduciary duties owed to Plaintiff and National Class members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

210. Defendant breached its fiduciary duties owed to Plaintiff and National Class members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.

211. Defendant breached its fiduciary duties owed to Plaintiff and National Class members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

212. Defendant breached its fiduciary duties owed to Plaintiff and National Class members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

213. Defendant breached its fiduciary duties to Plaintiff and National Class members by otherwise failing to safeguard Plaintiff's and National Class members' Private Information.

214. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and National Class members have suffered and will suffer injury, including but not limited to: (i) actual disruption of ongoing medical care and treatment; (ii) actual identity theft; (iii) the compromise, publication, or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains

in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vii) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and National Class members; and (viii) the diminished value of Defendant's services they received.

215. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and National Class members have suffered and will continue to suffer other forms of injury or harm, and other economic and non-economic losses.

Seventh Count

Willful Violation of the Fair Credit Reporting Act
(15 U.S.C. § 1681 *et seq.*)
(On Behalf of Plaintiff and National Class members)

216. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-122.

217. In enacting the FCRA, Congress made several findings, including that "there is a need to insure that consumer reporting agencies exercise grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy." 15 U.S.C. § 1681(a)(4).

218. The FCRA "require[s] that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information[.]" 15 U.S.C. § 1681(b).

219. The FCRA defines a "consumer reporting agency" as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in

the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f).

220. The FCRA defines a "consumer report" as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes; or any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1).

221. The FCRA defines "medical information" as "information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to the past, present, or future physical, mental, or behavioral health or condition of an individual; the provision of health care to an individual; or the payment for the provision of health care to an individual." 15 U.S.C. § 1681a(i).

222. Plaintiff's and National Class members' Personal Information, in whole or in part, constitutes "medical information" because it contains information that relates to the past, present, or future health of Plaintiff and National Class members, the provision of health care to Plaintiff and National Class members, or the payment for the provision of health care to Plaintiff and National Class members.

223. The FCRA specifically protects medical information, and restricts its dissemination to limited circumstances. *See, e.g.*, 15 U.S.C. §§ 1681a(d)(3); 1681b(g); and 1681(c)(a)(6).

224. Plaintiff's Personal Information constitutes a "consumer report" because the information bears on his character, reputation, personal characteristics, or mode of living, and is used and collected by Defendant for, among other things, determining Plaintiff's healthcare needs, determining the scope of and eligibility of Plaintiff's health or vision insurance coverage, and payments for Plaintiff's health care and eyewear purchases.

225. Defendant is a "consumer reporting agency" because, on a cooperative nonprofit basis or for monetary fees, Defendant regularly engages, in whole or in part, in the practice of assembling consumer information for the purpose of furnishing consumer reports to other parties, and it uses facilities of interstate commerce for the purpose of preparing or furnishing consumer reports.

226. As a Consumer Reporting Agency, Defendant was (and continues to be) required to adopt and maintain procedures designed to protect and limit the dissemination of consumer credit, personnel, insurance and other information (such as Plaintiff's and National Class members' Personal Information) in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. *See* 15 U.S.C. § 168l(b).

227. Defendant, however, willfully or recklessly violated the FCRA by failing to adopt, implement, and maintain adequate security measures to safeguard class members' Private Information by, among other things:

a. Failing to adequately monitor the security of their networks and systems;

b. Failure to periodically ensure that their appointment booking system had plans in place to maintain reasonable data security safeguards;

c. Allowing unauthorized access to class members' Private Information;

d. Failing to detect in a timely manner that class members' Private Information had been compromised; and

f. Failing to timely notify Plaintiff and class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

228. As a proximate result of Defendant's intentional or reckless violation of the FCRA and the resulting Data Breach, Plaintiff's and National Class members' Personal Information was accessed and stolen by unauthorized third parties in the public domain.

229. As a proximate result of Defendant's intentional or reckless violation of the FCRA and the resulting Data Breach, Plaintiff and National Class members were—and continue to be—damaged by the release, disclosure, and publication of their Personal Information, the loss of control of their Personal Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, emotional distress, anxiety, loss of privacy, and the loss of the benefit of the bargain they had struck with Defendant.

230. Plaintiff and National Class members are therefore entitled to compensation for their actual damages including, among other things, (i) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (ii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iii) deprivation of the value of their Personal Information, for which there is a well-established national and international market; (iv) anxiety and emotional distress; (v) statutory damages of not less than $100, and not more than $1000, each; and (vi) attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. § 1681n(a).

Eighth Count

Negligent Violation of the Fair Credit Reporting Act
(15 U.S.C. § 1681 *et seq.*)
(On Behalf of Plaintiff and National Class members)

231. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-122.

232. In enacting the FCRA, Congress made several findings, including that "there is a need to insure that consumer reporting agencies exercise grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy." 15 U.S.C. § 1681(a)(4).

233. The FCRA "require[s] that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information[.]" 15 U.S.C. § 1681(b).

234. The FCRA defines a "consumer reporting agency" as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f).

235. The FCRA defines a "consumer report" as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the

purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes; or any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1).

236. The FCRA defines "medical information" as "information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to the past, present, or future physical, mental, or behavioral health or condition of an individual; the provision of health care to an individual; or the payment for the provision of health care to an individual." 15 U.S.C. § 1681a(i).

237. Plaintiff's and National Class members' Personal Information, in whole or in part, constitutes "medical information" because it contains information that relates to the past, present, or future health of Plaintiff and National Class members, the provision of health care to Plaintiff and National Class members; or the payment for the provision of health care to Plaintiff and National Class members.

238. The FCRA specifically protects medical information, and restricts its dissemination to limited circumstances. *See, e.g.*, 15 U.S.C. §§ 1681a(d)(3); 1681b(g); and 1681(c)(a)(6).

239. Plaintiff's and the National Class members' Personal Information constitutes a "consumer report" because the information bears on his character, reputation, personal characteristics, or mode of living, and is used and collected by Defendant for, among other things, determining Plaintiff's healthcare needs, determining the scope of and eligibility of Plaintiff's health or vision insurance coverage, and payments for Plaintiff's health care and eyewear purchases.

240. Defendant is a "consumer reporting agency" because, on a cooperative nonprofit basis or for monetary fees, Defendant regularly engages, in whole or in part, in the practice of

assembling consumer information for the purpose of furnishing consumer reports to other parties, and it uses facilities of interstate commerce for the purpose of preparing or furnishing consumer reports.

241. As a Consumer Reporting Agency, Defendant was (and continues to be) required to adopt and maintain procedures designed to protect and limit the dissemination of consumer credit, personnel, insurance and other information (such as Plaintiff's and National Class members' Personal Information) in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. *See* 15 U.S.C. § 168l(b).

242. Defendant, however, negligently violated the FCRA by failing to adopt, implement, and maintain adequate security measures to safeguard class members' Private Information by, among other things:

a. Failing to adequately monitor the security of their networks and systems;

b. Failure to periodically ensure that their appointment booking system had plans in place to maintain reasonable data security safeguards;

c. Allowing unauthorized access to class members' Private Information;

d. Failing to detect in a timely manner that class members' Private Information had been compromised; and

f. Failing to timely notify Plaintiff and class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

243. As a proximate result of Defendant's negligent violation of the FCRA and the resulting Data Breach, Plaintiff's and National Class members' Personal Information was accessed and stolen by unauthorized third parties in the public domain.

244. As a proximate result of Defendant's negligent violation of the FCRA and the resulting Data Breach, Plaintiff and National Class members were—and continue to be—damaged by the release, disclosure, and publication of their Personal Information, the loss of control of their Personal Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, emotional distress, anxiety, loss of privacy, and the loss of the benefit of the bargain they had struck with Defendant.

245. Plaintiff and National Class members are therefore entitled to compensation for their actual damages including, among other things, (i) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (ii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iii) deprivation of the value of their Personal Information, for which there is a well-established national and international market; (iv) anxiety and emotional distress; and (v) attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. § 1681n(a).

Ninth Count

Violation of the Connecticut Unfair Trade Practices Act
(Conn. Gen. Stat. § 42-110a *et seq.*)
(On Behalf of Plaintiff and Connecticut Subclass members)

246. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-122.

247. The Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110a *et seq.*, prohibits unfair methods of competition and unfair practices in the conduct of trade or commerce.

248. Defendant is a "person" as defined by Conn. Gen. Stat. § 42-110a(3).

249. Defendant obtained Plaintiff's PII, and the PII of the Connecticut Subclass, through "trade" and "commerce" as defined by Conn. Gen. Stat. § 42-110a(3).

250. The Connecticut Unfair Trade Practices Act expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the Federal Trade Commission Act. *See* Conn. Gen. Stat. § 42-110b(b).

251. Defendant engaged in unfair business practices in violation of the Connecticut Unfair Trade Practices Act by, among other things, failing to implement and maintain reasonable security measures to protect its customers' PII, particularly in light of the heightened protections of PII mandated by HIPAA.

252. Specifically, Defendant committed unfair or deceptive acts and practices by:

a. failing to maintain adequate computer systems and data security practices to safeguard Private Information;

b. failing to disclose that its computer systems and data security practices were inadequate to safeguard Private Information from theft;

c. continued gathering and storage of PHI, PII, and other personal information after Defendant knew or should have known of the security vulnerabilities of its computer systems that were exploited in the Data Breach;

d. making and using false promises, set out in Defendant's Privacy Notice and Patient Rights, about the privacy and security of PHI, PII, and the Private Information of Plaintiff and Connecticut Subclass members;

e. deceptively misrepresenting the true nature and character of Defendant's data security practices, and;

f. continued gathering and storage of PHI, PII, and other personal information after Defendant knew or should have known of the cyberattack and Data Breach and before Defendant allegedly remediated the data security incident.

253. These unfair acts and practices violated duties imposed by laws, including but not limited to, the Federal Trade Commission Act, HIPAA, the FCRA, the Gramm- Leach-Bliley Act, and the Connecticut Unfair Trade Practices Act.

254. Defendant's conduct offends public policy as established by, among other things, the Federal Trade Commission Act, HIPAA, the FCRA, and the Gramm- Leach-Bliley Act, as well as the common law, and is within at least the penumbra of some common law, statutory or other established concepts of unfairness, is immoral, unethical, oppressive, or unscrupulous, and causes substantial injury to consumers.

255. Defendant's conduct caused substantial injury to Plaintiff and members of the Connecticut Subclass.

256. Defendant's conduct also harmed competition; while Defendant cut corners and minimized costs, its competitors spent the time and money necessary to ensure private information was appropriately secured and safeguarded.

257. Plaintiff and members of the Connecticut Subclass reasonably expected Defendant to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to protect and as necessary delete its customers' private personal and financial information.

258. The acts and omissions of Defendant were done knowingly and intentionally with the purpose of the sale of goods and services to Plaintiff and Connecticut Subclass members.

259. Plaintiff and Connecticut Subclass members were injured because: a) they would not have purchased medical care and treatment from Defendant had they known the true nature and character of Defendant's data security practices; b) Plaintiff and Connecticut Subclass members would not have entrusted their Private Information to Defendant in the absence of promises that Defendant would keep their information reasonably secure, and c) Plaintiff and Connecticut Subclass members would not have entrusted their Private Information to Defendant in the absence of the promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

260. As a direct and natural consequence of the violation of the Connecticut Unfair Practices Act, Plaintiff and Connecticut Subclass members suffered injury and all other damages including, but not limited to: (i) actual identity theft; (ii) the compromise, publication, or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Connecticut Subclass members; and (vii) the diminished value of Defendant's services they received.

Prayer for Relief

WHEREFORE, Plaintiff prays for judgment as follows:

a) Determining that this action is a proper class action;

b) Designating Plaintiff as a representative of the class and subclass under Federal Rule of Civil Procedure 23;

c) Designating Plaintiff's counsel as counsel for the class and subclass under Federal Rule of Civil Procedure 23;

d) Enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse or disclosure of Plaintiff's and class members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and the class members;

e) For equitable relief compelling Defendant to use appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;

f) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

g) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the class and subclass;

h) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

i) For an award of punitive damages, as allowable by law;

j) Awarding Plaintiff and the class and subclass reasonable attorneys' fees, costs, and expenses under Rule 23 of the Federal Rules of Civil Procedure and the FCRA;

k) Awarding Plaintiff and the members of the class and subclass any pre-judgment and post-judgment interest as may be allowed under the law; and

l) Awarding such other and further relief as the Court may deem just and proper.

Jury Trial Demand

Plaintiff demands a jury trial on all issues so triable.

Dated: November 10, 2020

Respectfully submitted,

/s/ Ronald S. Weiss
Ronald S. Weiss, Attorney & Counselor
6725 West Central Ave., M310
Toledo, OH 43617
Phone: 248-737-8000
ron@ronweissattorney.com

GREENWALD DAVIDSON RADBIL PLLC
Michael L. Greenwald*
7601 N. Federal Hwy., Suite A-230
Boca Raton, Florida 33487
Phone: 561.826.5477
mgreenwald@gdrlawfirm.com

* to seek admission pro hac vice