Exhibit D

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF OHIO

In re LUXOTTICA OF AMERICA, INC. DATA SECURITY BREACH LITIGATION This Document Relates To: ALL ACTIONS.	No. 1:20-cv-00908-MRB (Consolidated with Case Nos. 1:20-cv-00983 & 1:20-cv-01011) **CLASS ACTION** Judge Michael R. Barrett Magistrate Judge Karen L. Litkovitz

PLAINTIFFS' CONSOLIDATED CLASS ACTION COMPLAINT
DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Page

Plaintiff Jessie Crockett ("Crockett"), Michael Doyle ("Doyle"), Phillip Gervais ("Gervais"), John Gloss ("Gloss"), Larry Payne ("Payne"), on behalf of his minor child M.P. ("M.P."), and Donna Rivera ("Rivera") (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, through their undersigned counsel, allege as follows against defendant Luxottica of America, Inc. ("Luxottica" or "Defendant"), based upon personal knowledge as to themselves and, as to all other matters, upon information and belief, including their counsel's investigation. Plaintiffs believe additional evidentiary support exists for their allegations, given an opportunity for discovery.

I. INTRODUCTION

1. This class action arises out of a recent cyberattack and data breach ("Data Breach") involving Luxottica's network of eye care centers.

2. 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."

3. Luxottica is responsible for allowing the Data Breach to occur because it failed to implement and maintain reasonable safeguards and failed to comply with industry-standard data security practices as well as federal and state laws and regulations governing data security, including security of protected health information ("PHI").

4. During the duration of the Data Breach, Luxottica failed to, among other things, detect that ill-intentioned criminals had accessed its computer data and storage systems, notice the massive amounts of data that were compromised, and take any steps to investigate the red flags that should have warned Luxottica that its systems were not secure. Had Luxottica properly monitored its information technology infrastructure, it would have discovered the intrusion sooner.

5. Luxottica had obligations created by, among other things, The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), federal and state regulations regarding data security and PHI security, industry standards, and common law to keep their personal identifiable information ("PII"), including PHI, confidential and to protect it from unauthorized access and disclosure.

6. PII compromised in the Data Breach includes names, demographic information, dates of birth, Social Security numbers, health insurance information, medical information, other PHI as defined by HIPAA, and additional PII that Luxottica collected and maintained.

7. Plaintiffs and class members provided their PII and PHI to Luxottica with the reasonable expectation and mutual understanding that Luxottica would comply with its obligations to keep such information confidential and secure from unauthorized access.

8. Luxottica's data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the healthcare industry preceding the date of the Data Breach.

9. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and class members' PII and PHI, Luxottica assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and class members' PII and PHI from disclosure.

10. Plaintiffs and class members have taken reasonable steps to maintain the confidentiality of their PII and PHI.

11. Plaintiffs and class members relied on Luxottica to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

12. As a result of Luxottica's failure to protect the PII and PHI it was entrusted with, Plaintiffs' and class members' PII and PHI were accessed by malicious cyber criminals. Plaintiffs and class members therefore have been exposed to and/or are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. They also 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 Data Breach. Plaintiffs and class members have also lost the inherent value of their PII and PHI. This harm was compounded by Luxottica's failure to ensure that patients of its eye care centers received proper and timely notification of the Data Breach.

13. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence; (ii) negligence per se; (iii) declaratory judgment; (iv) breach of confidence; (v) unjust enrichment; (vi) breach of fiduciary duty; (vii) violations of the Fair Credit Reporting Act, 15 U.S.C. §1681, *et seq*. ("FCRA"); (viii) violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, *et seq.* ("UCL"); (ix) violation of the California Customer Records Act, Cal. Civ. Code §1798.80, *et seq.* ("CCRA"); (x) violation of the California Consumer Privacy Act, Cal. Civ. Code §1798.100, *et seq.* ("CCPA"); (xi) violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code §56, *et seq.* ("CMIA"); (xii) violation of the Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. §42-110a, *et seq*. ("CUTPA"); (xiii) violation of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §501.201, *et seq.* ("FDUTPA"); (xiv) and violation of the Missouri Merchandising Practices Act, Mo. Stat. §407.020(1), *et seq.* ("MMPA").

II. PARTIES

14. Plaintiff Phillip Gervais is a natural person who at all relevant times resided in and is a citizen of Santa Clara County, California. Mr. Gervais made an appointment and received eye

healthcare treatment from Target Optical, one of Luxottica's eye care centers. Mr. Gervais has been a patient at Target Optical located at 2004 El Camino Real, Santa Clara, CA 95050, since May 2018 and has made various appointments through the Scheduling Application. Mr. Gervais has obtained various services, including annual vision exams, from Target Optical. He has paid co-pays for these services, including a recent copay for an annual vision exam on October 3, 2020. He entrusted PII, including PHI, and other confidential information such as contact information, vision insurance policy information, medical history, and debit card information, to Luxottica with the reasonable expectation and understanding that Luxottica would protect, maintain, and safeguard that information from compromise, unauthorized disclosure, and misuse by unauthorized users, and would be timely notified of any data security incidents involving his PII and PHI should such occur. Had Mr. Gervais known that Defendant did not take appropriate measures to secure his PII and PHI, Mr. Gervais would not have provided his PII and PHI to Defendant, and would have sought vision services from a different company. Other than fraudulent charges on an unrelated debit card over ten years ago, Mr. Gervais has not previously been a victim of fraud or identity theft. Nor is Mr. Gervais aware of any of his PII or PHI being compromised in other data breaches. Mr. Gervais received a Notice of Data Breach from Luxottica dated October 28, 2020. The Notice informed Mr. Gervais that the following PII and PHI were compromised in the Data Breach: his "full name, contact information, appointment date and time, and doctor or appointment notes that may indicate information related to eye care treatment, such as prescriptions, health conditions, or procedures." Since learning about the Data Breach at the end of October 2020, he has suffered emotional anguish and distress, including but not limited to anxiety related to the breach of his sensitive PII and PHI. As a result of the Data Breach, Mr. Gervais estimates that he has spent at least one hour monitoring his credit score and conducting internet research regarding the scope of the breach and the information compromised.

15. Plaintiff Michael Doyle is a natural person who at all relevant times resided in and is a citizen of New London County, Connecticut. Mr. Doyle receives vision insurance through EyeMed. Mr. Doyle has been a patient at Pearle Vision, one of Luxottica's eye care centers, since 2014, and he has typically made appointments by telephone, and received confirmation and follow-up communications by email. On or about July 2020, Mr. Doyle visited a Pearle Vision optometrist at 909 Hartford Turnpike, Waterford, CT 06385 to obtain an annual vision exam and purchase new prescription glasses. As part of this process, Mr. Doyle provided his Social Security number, EyeMed vision insurance information, and relevant medical history to Defendant or Defendant's employees. He entrusted PII, including PHI, and other confidential information such as contact information, health insurance policy information, prescription information, medical conditions, and Social Security number, to Luxottica with the reasonable expectation and understanding that Luxottica would protect, maintain, and safeguard that information from compromise, unauthorized disclosure, and misuse by unauthorized users, and would be timely notified of any data security incidents involving his PII should such occur. Mr. Doyle received a Notice of Data Breach from Luxottica dated October 28, 2020. The Notice informed Mr. Doyle that the following PII and PHI were compromised in the Data Breach: his "full name, contact information, appointment date and time, and health insurance policy number." Had Mr. Doyle known that Defendant did not take appropriate measures to secure his PII and PHI, Mr. Doyle would not have provided his PII and PHI to Defendant, and would have sought vision services from a different company. In addition, prior to acquiring his new eyeglasses, Mr. Doyle believes that he submitted a cash payment of approximately $150 as a deposit for his new eyeglasses, followed by a final payment of approximately $200, totaling approximately $350 in payments to Defendant. As a result of the Data Breach, Mr. Doyle estimates that he has spent at least one hour

responding to the Data Breach after receiving notice from Luxottica, including discussing the impact of the Data Breach with his attorneys.

16. Plaintiff Jessie Crockett is a natural person and a resident and citizen of the State of Wisconsin. She and her family use Pearle Vision, one of Luxottica's eye care centers, at 3063 Meadowlark Lane, Altoona, Wisconsin 54720 for their eye care needs, including using the Scheduling Application to obtain appointments and eye care, such as eye exams and glasses. Plaintiff Crockett entrusted her PII, PHI, and other confidential information such as contact information, health insurance policy information, prescription information, medical conditions, and Social Security number, to Luxottica with the reasonable expectation and understanding that Luxottica would take, at a minimum, industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her PII and PHI. Plaintiff Crockett was required by Luxottica to verify appointments with her Social Security number. Since learning about the breach at the end of October 2020, she has suffered emotional anguish and distress, including but not limited to anxiety and lost sleep related to the breach of her sensitive personal, financial, and health information, as well as the breach of her minor son's sensitive personal, financial, and health information (which was also compromised in the breach). As a result of the breach and anxiety it has caused, she estimates that she spends at least 15 minutes per day reviewing her credit, and reviews it several times a day; before the breach, she would only review her credit once every week or two. She also often conducts deep reviews of her credit and financial account information, commonly exceeding seven hours per week. Prior to the breach, she typically only reviewed her credit information once a month. Furthermore, following the breach, she believes she receives on average about 15 scam and telemarketing calls per day. Following the breach, Plaintiff Crocket also signed up for bank card and credit card monitoring through True Bill, but she regularly worries

that this is not enough, and that she may have to pay much more for additional credit and ID monitoring. Plaintiff Crocket is in daily fear of someone messing up her credit, using her PII or PHI, or stealing her identity and accruing debt under her name.

17. Plaintiff John Gloss is a natural person who at all relevant times resided in and is a citizen of St. Louis County, Missouri. Mr. Gloss receives vision insurance through EyeMed, which he paid $9.37 per month from at least July 2019 through June 2020. On or about July 2020, Mr. Gloss used the Scheduling Application to book an optometrist appointment through LensCrafters, another Luxottica eye care center, which referred him to Cunningham Vision Care at 92 Chesterfield Mall, Chesterfield, MO 63017. Mr. Gloss booked this appointment to obtain an annual vision exam and purchase new prescription eyeglasses. As part of this process, Mr. Gloss provided his EyeMed vision insurance information, and relevant medical history to Defendant or Defendant's employees. Mr. Gloss does not recall if he also provided his Social Security number to Defendant or Defendant's employees. On or about November 30, 2020, Mr. Gloss received an email from Defendant informing him about the Data Breach. The Notice informed Mr. Gloss the following PII and PHI were compromised in the Data Breach: his "full name, contact information, appointment date and time, and health insurance policy number." Following Notice of the Data Breach, Mr. Gloss spent approximately four hours examining his bank statements and credit accounts to ensure that his PII and PHI had not already been used by a third party. Had Mr. Gloss known that Defendant did not take appropriate measures to secure his PII and PHI, Mr. Gloss would not have provided his PII and PHI to Defendant, and he would have sought vision services from a different company. In fact, as a result of Mr. Gloss's frustration with Defendant's failure to protect his PII and PHI, he spent approximately two hours researching data privacy laws and requirements, and another two hours trying to contact Cunningham Vision Care to request that they remove all of his PII and PHI from their database. However, an employee at Cunningham

Vision Care stated that it would be unable to remove his PII and PHI, and instead could only set his account to an "inactive" status.

18. Plaintiff Donna Rivera is a natural person and resident and citizen of the State of Ohio. Plaintiff and her family have made appointments using the Scheduling Application and received eye care treatment from the LensCrafters, one of Luxottica's eye care centers, at 3580 Westgate, Fairview Park, Ohio 44126. She entrusted her PII, PHI, and other confidential information such as health savings account ("HSA") credit card data, to Luxottica with the reasonable expectation and understanding that Luxottica would take, at a minimum, industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her PII and PHI. Since she was informed on or around November 30, 2020, that a substantial amount of her PII and PHI was compromised, she has suffered emotional anguish and the loss of a substantial amount of her time. She suffers regular anxiety knowing her PII and PHI is available for purchase by bad actors. She feels as if she is constantly just waiting for the other shoe to drop, but she also knows that it might be tomorrow or years when someone misuses her PII and PHI. She has spent hours reading up on the Data Breach, including reading sources that suggest Luxottica has not been forthright in the total number of Social Security numbers breached. She spends hours every week trying to read as much as possible about, and even reached out to a professional group that uses its resources to take down scammers, to see if they could help understand whether any of her or others' PII and PHI taken in the Data Breach might have been sold and used. That group referred her to private investigators, but she did not seek their services because of the prohibitive cost. She reads for hours a week as an attempt to quell her anxiety. Soon after the Data Breach, Plaintiff Rivera signed up for credit and identity theft monitoring services, for which she pays $19.99 per month. She spends time looking at her bank statement every day and, with her husband, monitors their

HSA account. She monitors her credit through multiple sources, checking as often as she can. Before the Data Breach, she did not check her credit more than once or twice a year. Plaintiff Rivera has seen a significant uptick in unwanted spam telephone calls since the Data Breach, and she has had to take the time to send the telephone information to the Federal Trade Commission ("FTC"). She is most scared that someone will steal her identity.

19. Plaintiff Larry Payne is a natural person, father of M.P., and both are residents and citizens of the State of Florida. M.P. is a minor child. M.P. received services at the Target Optical located at 4795 West Irlo Bronson Memorial Highway, Kissimmee, FL 34746, and his PII and PHI were entrusted to the clinic. Luxottica was the service provider for the clinic, at which M.P. received services and which received M.P.'s PII and PHI. Plaintiff Larry Payne paid Defendant money for the eyecare services received by M.P. Larry Payne received notice of the Data Breach dated November 13, 2020, on behalf of M.P. Luxottica stated in its notice that M.P.'s personal information was compromised, including his name and other identifying information. M.P. has suffered injury directly and proximately caused by the Data Breach, including: (a) compromise of M.P.'s valuable PII and PHI; (b) the imminent and certain impeding injury flowing from fraud and identity theft posed by M.P.'s PII and PHI being placed in the hands of, bought, sold, and used by cyber criminals; (c) damages to and diminution in value of M.P.'s PHI and PII, entrusted to Defendant for the sole purpose of obtaining necessary medical products and services, with the understanding and expectation that Defendant would guard this information against disclosure; and (d) continued risk to M.P.'s PII and PHI, which remain in the possession of Defendant and which are subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect M.P.'s PII and PHI.

20. Luxottica is an Ohio corporation with its principal place of business in Mason, Ohio. It is the subsidiary of Luxottica Group S.p.A., an Italian eyewear conglomerate. Luxottica was formerly known as Luxottica Retail North America Inc.

III. JURISDICTION AND VENUE

21. This Court has federal question subject matter jurisdiction over this action pursuant to 28 U.S.C. §1331 because Plaintiffs assert claims that necessarily raise substantial disputed federal issues under HIPAA, the FTC Act (15 U.S.C. §45) ("FTC Act"), the Gramm-Leach-Bliley Act (15 U.S.C. §6801), and the FCRA (15 U.S.C. §1681, *et seq.*).

22. This Court also has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because putative class members are citizens of a different state than Luxottica.

23. This Court has personal jurisdiction over Luxottica because it is authorized to conduct and does regularly conduct business in Ohio and is headquartered in Mason, Ohio.

24. Venue is proper in this District under 28 U.S.C. §1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Luxottica and Its Privacy and Data Security Representations

25. Luxottica touts that it is "a market leader in the design, manufacture and distribution of fashion, luxury, sports and performance eyewear."[1] As of December 31, 2019, Luxottica

[1] LUXOTTICA, http://www.luxottica.com/en (last visited Jan. 22, 2021).

operated a total of 3,849 corporate stores in North America, including multiple Target Optical locations throughout the United States.[2]

26. Luxottica produces and licenses eyewear under numerous brand names, including Coach, Chanel, Dolce & Gabbana, Oakley, Prada, and Ray-Ban, among others.[3] It also operates various retail brands, including LensCrafters, Pearle Vision, Sunglass Hut, and Target Optical.[4] In addition, Luxottica 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."[5]

27. Luxottica provides optometry and vision services to customers in connection with some of its retail operations (*i.e.*, eye healthcare providers), including Target Optical, LensCrafters, and Pearle Vision. In the ordinary course of receiving treatment and health care services from Luxottica, optometry and vision service customers ("Patients") are required to provide contact information (including, but not limited to, name, email, and shipping address) and financial information (including, but not limited to, credit card number, expiration date, etc.). Patients also must provide their date of birth, insurance information and coverage, and other PII or PHI that may be deemed necessary to provide care.

---

[2] Tugba Sabanoglu, *Total number of stores of Luxottica in North America in 2019, by brand**, STATISTA (Nov. 30, 2020), https://www.statista.com/statistics/241663/number-of-stores-of-luxottica-in-north-america/#:~:text=As%20of%20December%2031%2C%202019,corporate%20stores%20in%20North%20America; Optical, TARGET, https://local.targetoptical.com/ (last visited Jan. 22, 2021).

[3] *Eyewear Brands: Our Glasses*, LUXOTTICA, http://www.luxottica.com/en/eyewear-brands (last visited Jan. 22, 2021).

[4] *Retail Brands*, LUXOTTICA, http://www.luxottica.com/en/retail-brands (last visited Jan. 22, 2021).

[5] Retail Brands, *EyeMed Vision Care*, LUXOTTICA http://www.luxottica.com/en/retail-brands/eyemed-vision-care (last visited Jan. 22, 2021).

28. Luxottica also gathers certain medical information, including PHI, about Patients and creates records of the care it provides them.

29. Additionally, Luxottica may receive PII and PHI on its Patients from other individuals and/or organizations that are part of a Patient's "circle of care," such as referring physicians, Patients' other doctors, Patients' plan(s), close friends, and/or family members.

30. All of Luxottica's current and future affiliates and other brands may share Patient information with each other for various purposes.

31. In the course of treating Patients, Luxottica acquires, collects, and stores or processes a massive amount of PII, including PHI, on its Patients, including: (1) contact information (including, but not limited to, name, email, and shipping address); (2) financial information (including, but not limited to, credit card number, expiration date, etc.); (3) insurance information; and (4) medical history.

32. As a condition of receiving healthcare services from Luxottica, Luxottica requires that its Patients entrust it with highly sensitive PII, including PHI.

33. Luxottica is fully aware of the sensitive nature of Patients' PII and PHI that it collects and stores on or processes through its systems.

34. Luxottica's HIPAA Notice provides that it collects PHI from Patients "for treatment, to obtain payment for treatment, for administrative purposes, and to evaluate the quality of care and service that you receive."[6] It further provides that, "[y]our health information is contained in a medical or optical dispensary record that is the physical property of Luxottica Retail.[7] Your health information consists of any information, whether in oral or recorded form,

[6] Optical, TARGET https://web.archive.org/web/20170619102139/http://www.targetoptical.com/to-us/content/hipaa (last visited Jan. 22, 2021).

[7] Luxottica is formerly known as Luxottica Retail North America Inc.

that is created or received by us and individually identifies you, and that relates to your past, present or future physical or mental health or condition; the provision of health care to you; or the past, present or future payment for the provision of health care to you."[8]

35. Recognizing the sensitivity of the PHI it maintains, Luxottica's HIPAA Notice states that it is "committed to protecting your privacy," and that it is "required by applicable federal and state law to . . . [m]aintain the privacy and safeguard the security of your health information; [and] notify you, along with all other affected individuals, of a breach of unsecured health information."[9]

36. Luxottica's HIPAA Notice specifically sets forth expectations for Luxottica's behavior in the event of a data breach, providing that if Luxottica "discover[s] that your health information has been breached (for example, disclosed to or acquired by an unauthorized person, stolen, lost, or otherwise used or disclosed in violation of applicable privacy law) 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."

B. Luxottica's Knowledge That It Was and Is a Target of Cyber Threats

37. Luxottica knew it was a prime target for hackers given the significant amount of sensitive Patient PII and PHI processed through its computer data and storage systems, including the Scheduling Application.

38. Through EyeMed, Luxottica processed employer and payment information, in addition to all the information about vision, vision healthcare, and any other information that it might demand as a benefits provider, such as Social Security number, age, gender, and prior health history.

---

8 TARGET, *supra* note 6.

9 *Id.*

39. Through Luxottica's eye care providers such as LensCrafters, Pearle Vision, and Target Optical, Luxottica possesses information provided to or from insurers, such as Social Security numbers, as well as medical information, such as current and prior health history, history of treatment and examinations, HSA information, credit and debit card and other payment information, email and home addresses, and other PII and PHI.

40. Through retail establishments such as Ray-Ban, Sunglass Hut, and Oakley, Luxottica processed credit card and other personal information, as well as data related to predicting consumers' preferences.

41. Experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI that they collect and maintain.

42. Luxottica's knowledge is underscored by the massive number of data breaches, including those perpetrated against the healthcare sector, that have occurred in recent years. Over 41 million patient records were breached in 2019, with a single hacking incident affecting close to 21 million records.[10] Healthcare data breaches in 2019 almost tripled those the healthcare industry experienced in 2018 when 15 million patient records were affected by data breach incidents, according to a report from Protenus and DataBreaches.net.[11]

43. Protenus, a healthcare compliance analytics firm, analyzed data breach incidents disclosed to the U.S. Department of Health and Human Services or the media during 2019, finding there has been an alarming increase in the number of breaches of patient privacy since 2016, when

[10] Heather Landi, *Number of patient records breached nearly triples in 2019*, FIERCE HEALTHCARE (Feb. 20, 2020), https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats (last visited Jan. 22, 2021).

[11] *Id.*; *see also* Resources, *2020 Breach Barometer*, PROTENUS, https://www.protenus.com/resources/2020-breach-barometer/ (last visited Jan. 22, 2021).

there were 450 security incidents involving patient data.[12] In 2019, that number jumped to 572 incidents, which is likely an underestimate, as two of the incidents for which there were no data affected 500 dental practices and clinics and could affect significant volumes of patient records. There continues to be at least one health data breach per day.[13]

44. Indeed, Luxottica subsidiary EyeMed discovered that it was the victim of a separate data breach one month ***before*** the Data Breach at issue in this litigation, yet Luxottica inexplicably did not take the steps necessary to prevent the Data Breach.[14] And Luxottica itself appears to have suffered a cyber-attack in 2008 in which hackers stole the personal information of over 59,000 employees.[15]

45. Despite knowing the prevalence of these healthcare data breaches, including a recent breach directly affecting its own subsidiary EyeMed, Luxottica failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to their highly sensitive systems and databases. Luxottica had the resources to prevent a breach, but it neglected to adequately invest in data security, despite the growing number of well-publicized data breaches affecting the healthcare industry.

46. Luxottica failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures to ensure that similar vulnerabilities were avoided or remedied and that Plaintiffs' and class members' PII and PHI were protected.

---

[12] *Id.*

[13] *Id.*

[14] *Notice of Security Incident*, EYEMED, https://eyemed.com/en-us/notice (last visited Jan. 22, 2021).

[15] Richard Adhikari, *Mainframe Breach at LensCrafters Parent Hits 59K*, INTERNETNEWS (Nov. 26, 2008), http://www.internetnews.com/security/article.php/3787431/Mainframe+Breach+at+LensCrafters+Parent+Hits+59K.htm.

C. The Data Breach

47. On August 9, 2020, Luxottica allegedly learned that on or about August 5, 2020, an unauthorized person "accessed the Luxottica-managed" Scheduling Application.[16] According to Luxottica, upon learning of the Data Breach, it "contained it, and immediately began an investigation to determine the extent of the incident." On August 28, 2020, Luxottica preliminarily concluded that the attacker might have accessed and acquired patient information.[17] While Luxottica informed its customers that the Data Breach originated from the Scheduling Application, the method of the Data Breach still has not been disclosed.

48. Despite having knowledge of the Data Breach no later than August 9, 2020, and warranting to consumers in its HIPAA 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," Luxottica did not issue a "Security Incident" notification until October 28, 2020, nor did it notify affected Patients until October 28, 2020, or later.[18]

49. The Security Incident notification disclosed that the PII and PHI accessed in the Data Breach may have included: "full name, contact information, appointment date and time, health insurance policy number, and doctor or appointment notes that may indicate information related to eye care treatment, such as prescriptions, health conditions or procedures."[19] The

---

[16] *Important Information Regarding Security Incident*, LUXOTTICA, https://luxottica.kroll.com/ (last visited Jan. 22, 2021).

[17] *Id.*

[18] *Id.*

[19] *Id.*

Security Incident notification also stated that "[i]n a limited number of cases, Social Security numbers and credit card numbers were impacted."[20]

50. Luxottica reported to the U.S. Department of Health and Human Services that the Data Breach compromised the PII of at least 829,454 Patients.[21]

51. While Luxottica 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 and advised victims of the Data Breach, including Plaintiffs, to "remain vigilant, including by regularly reviewing your account statements." Luxottica advised that Patients who had their health information compromised should "take steps to protect themselves, for example by closely monitoring notices from your health insurer and health care providers for unexpected activity."[22]

52. Further, this consumer Data Breach coincides with a ransomware cyberattack in September 2020 involving Luxottica's parent company, Luxottica Group S.p.A., in which "some of the web sites operated by [Luxottica] were not reachable, including Ray-Ban, Sunglass Hut, LensCrafters, EyeMed, and Pearle Vision."[23]

53. Thereafter, a "huge trove of files" was posted on the dark web, "related to the personnel office and finance departments," of Luxottica Group S.p.A.[24] The cybercriminals

---

[20] *Id.*

[21] Office for Civil Rights, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, HHS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Jan. 22, 2021).

[22] *Important Information Regarding Security Incident*, *supra* note 16.

[23] Pierluigi Paganini, *Hackers hit Luxottica, production stopped at two Italian plants*, SEC. AFFAIRS (Sept. 22, 2020), https://securityaffairs.co/wordpress/108611/cyber-crime/luxottica-cyber-attack.html.

[24] Pierluigi Paganini, Nefilim ransomware gang published Luxottica data on its leak site, SEC. AFFAIRS (Oct. 20, 2020), https://securityaffairs.co/wordpress/109778/data-breach/luxottica-data-leak-ransomware.html; *see also* Sam Varghese, *Eyewear giant Luxottica hit by Windows Nefilim ransomware, data leaked*, ITWIRE (Oct. 20, 2020), https://www.itwire.com/security/eyewear-giant-luxottica-hit-by-windows-nefilim-ransomware,-data-leaked.html.

behind the initial ransomware attack leaked the exfiltrated data online in installments, with the first containing "financial information and human resource documents" and the last showing "banking information and other sensitive data."[25]

54. Cybersecurity intelligence firm Bad Packets posited that the cause of the ransomware attack was "a Citrix ADX controller device vulnerable to the critical CVE-2019 19781 flaw."[26]

55. As a result, Luxottica and its international parent company have apparently suffered two serious data breaches in as many months, indicating systemic problems in Luxottica's cybersecurity practices.

56. When considering that "[r]ansomware groups frequently buy access to compromised networks from the hackers that compromised them," it is "not at all surprising that a compromise would result in more than one type of security incident."[27]

57. Because of the nature of the PII and PHI stored or processed by Luxottica, Plaintiffs understand that all categories of PII and PHI were subject to unauthorized access and exfiltration, theft, or disclosure. In other words, criminals would have no purpose for hacking Luxottica other than to exfiltrate or steal the coveted PII and PHI stored or processed by Luxottica.

58. Luxottica's response to the Data Breach caused confusion among the victims of the Data Breach, resulting in Plaintiffs and class members spending time, and continuing to spend a

---

[25] Jessica Davis, *UPDATE: Luxottica Data Leaked by Hackers After Ransomware Attack*, HEALTH IT SEC., https://healthitsecurity.com/news/luxottica-data-leaked-by-hackers-after-ransomware-attack-breach (last visited Jan. 22, 2021).

[26] Lawrence Abrams, *Ray-Ban owner Luxottica confirms ransomware attack, work disrupted*, BLEEPING COMPUTER (Sept. 22, 2020), https://www.bleepingcomputer.com/news/security/ray-ban-owner-luxottica-confirms-ransomware-attack-work-disrupted/.

[27] *See supra* note 25.

significant amount of time into the future, taking measures to protect themselves from identity theft, fraud, and other identity-related crimes.

59. Luxottica is responsible for allowing the Data Breach to occur because it failed to implement and maintain any reasonable safeguards and failed to comply with industry-standard data security practices, contrary to state and federal laws and regulations and its own duties to protect its Patients' PII and PHI.

60. As a result of Luxottica's failure to protect the sensitive PII and PHI it was entrusted with, Plaintiffs and class members are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. Plaintiffs and class members have also lost the inherent value of their PII.

61. Plaintiffs and class members provided their PII and PHI to Luxottica with the expectation and understanding that Luxottica would adequately protect and store their data. If Plaintiffs and class members had known that Luxottica's data security was insufficient to protect their PII and PHI, they would have demanded that their eye care center not store or process their PII and PHI through Luxottica's computer data and storage systems.

D. Luxottica Failed to Comply with Statutory and Regulatory Obligations

62. Luxottica had obligations created by HIPAA, the FTC Act, industry standards, and common law to keep Plaintiffs' and class members' PII and PHI confidential and to protect it from unauthorized access and disclosure.

63. Luxottica is an entity covered by HIPAA (45 C.F.R. §160.102). As such, it is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

64. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

65. HIPAA's Security Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is held or transferred in electronic form.

66. HIPAA requires Luxottica to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. §164.302.

67. "Electronic protected health information" is "individually identifiable health information . . . that is (i) Transmitted by electronic media; maintained in electronic media." 45 C.F.R. §160.103.

68. HIPAA's Security Rule requires Luxottica to do the following:

(a) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

(b) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

(c) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

(d) Ensure compliance by its workforce.

69. HIPAA also required Luxottica to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. §164.306(e).

70. HIPAA also required Luxottica to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. §164.312(a)(1).

71. The HIPAA Breach Notification Rule, 45 C.F.R. §§164.400-414, also required Luxottica to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

72. Luxottica was also prohibited by the FTC Act (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

73. Moreover, federal agencies have issued recommendations and guidelines to temper data breaches and the resulting harm to individuals and financial institutions. For example, the FTC has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[28]

74. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[29] Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no

[28] *Start with Security, A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[29] *Protecting Personal Information, A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[30]

75. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[31]

76. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. §45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[32]

77. Luxottica is also required by the CCRA, the CMIA, and various other states' laws and regulations to protect Plaintiffs' and class members' PII and PHI, and further, to handle any breach of the same in accordance with applicable breach notification statutes.

---

[30] *Id.*

[31] *Start with Security*, *supra* note 28.

[32] *Privacy and Security Enforcement: Press Releases*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Jan. 22, 2021).

78. In addition to their obligations under federal and state laws, Luxottica owed a duty to Plaintiffs and class members whose PII and PHI were entrusted to Luxottica to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Luxottica owed a duty to Plaintiffs and class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its systems and networks adequately protected the PII and PHI of Plaintiffs and class members.

79. Luxottica owed a duty to Plaintiffs and class members whose PII and PHI were entrusted to Defendant to design, maintain, and test its systems to ensure that the PII and PHI in Defendant's possession were adequately secured and protected.

80. Luxottica owed a duty to Plaintiffs and class members whose PII and PHI were entrusted to Defendant to create and implement reasonable data security practices and procedures to protect the PII and PHI in their possession.

81. Luxottica owed a duty to Plaintiffs and class members whose PII and PHI were entrusted to Luxottica to implement processes that would detect a breach on its data security systems in a timely manner.

82. Luxottica owed a duty to Plaintiffs and class members whose PII and PHI were entrusted to Defendant to act upon data security warnings and alerts in a timely fashion.

83. Luxottica owed a duty to Plaintiffs and class members whose PII and PHI were entrusted to Luxottica to disclose if its systems and data security practices were inadequate to safeguard individuals' PII and PHI from theft because such an inadequacy would be a material fact in the decision to entrust PII and PHI with Luxottica.

84. Luxottica owed a duty to Plaintiffs and class members whose PII and PHI were entrusted to Defendant to disclose in a timely and accurate manner when data breaches occurred.

85. Luxottica owed a duty of care to Plaintiffs and class members because they were foreseeable and probable victims of any inadequate data security practices.

86. In this case, Luxottica was fully aware of its obligation to use reasonable measures to protect the PII and PHI of its customers, acknowledging as much in its HIPAA Notice. Luxottica also knew it was a target for hackers. But despite understanding the consequences of inadequate data security, Luxottica failed to comply with industry-standard data security requirements.

87. Luxottica's failure to employ reasonable and appropriate measures to protect against unauthorized access to Patients' PII and PHI constitute an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. §45, and various state consumer protection and data breach statutes.

E. Effect of the Data Breach

88. Luxottica's failure to keep Plaintiffs' and class members' PII and PHI secure has severe ramifications. Given the sensitive nature of the PII and PHI compromised in the Data Breach, cyber criminals can commit identity theft and other identity-related fraud against Plaintiffs and class members now and into the indefinite future.

89. The information compromised included PHI, which "can fetch up to $350 on the dark web."[33] Stolen PHI is a one of the most valuable commodities on the criminal information black market. In 2014, the FBI warned healthcare organizations that PHI data is worth 10 times the amount of personal credit card data on the black market.[34] PHI data for sale is so valuable

[33] *How Cybercriminals Make Money: How much is your information worth to a cybercriminal via the Dark Web?*, KEEPER SEC., https://www.keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html (last visited Jan. 22, 2021).

[34] Stolen PHI health credentials can sell for up to 20 times the value of a U.S. credit card number, according to Don Jackson, director of threat intelligence at PhishLabs, a cyber-crime protection company who obtained this data by monitoring underground exchanges where cyber-criminals sell the information. *See* William Maruca, *Hacked Health Records Prized for their Black Market*

because PHI information is so broad, and it can therefore be used for a wide variety of criminal activity such as to create fake IDs, buy medical equipment and drugs that can be resold on the street, or combine patient numbers with false provider numbers to file fake claims with insurers. As explained by the FTC, "[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."[35]

90. Indeed, Luxottica itself recognized this risk when it instructed victims of the Data Breach to "take steps to protect themselves, for example by closely monitoring notices from your health insurer and health care providers for unexpected activity."[36]

91. The value of Plaintiffs' and the class members' PHI on the black market is considerable. Stolen PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" Internet websites, making the information publicly available, for a substantial fee.

92. It can take patients years to spot healthcare identity or PHI theft, giving criminals plenty of time to exploit that information for as much cash as possible. That is exactly why medical data PHI is more desirable to criminals than credit card theft. Credit card or financial information

---

Value, HIPAA & HEALTH INFO. TECH., FOX ROTHSCHILD LLP (Mar. 15, 2015) *https://hipaahealthlaw.foxrothschild.com/2015/03/articles/articles/hacked-health-records-prized-for-their-black-market-value/#:~:text=Medscape%20reports%20that%20a%20stolen,number%20or%20credit%20card%20number*. Dark web monitoring is a commercially available service which, at a minimum, Luxottica can and should perform (or hire a third-party expert to perform).

[35] *See Medical Identity Theft*, FTC, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Jan. 22, 2021).

[36] *Important Information Regarding Security Incident*, *supra* note 16.

theft can be spotted by banks early on, and accounts can be quickly frozen or cancelled once the fraud is detected, making credit card and financial data much less valuable to criminals than PHI.

93. Luxottica has disclosed and given access to the PHI of Plaintiffs and class members for criminals to use in the conduct of criminal activity. Specifically, Luxottica has opened up, disclosed, and exposed the contact information and PHI of Plaintiffs and class members to persons engaged in disruptive and unlawful business practices and tactics, including spam and "phishing" emails, robo-dialed calls, junk texts and faxes, other unwanted calls and communications, online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (*i.e.*, identity fraud), all using compromised PHI.

94. In recognition of the value of PHI, today a growing number of legitimate companies are developing business models that center on giving consumers a choice on whether or not they themselves wish to monetize (*i.e.*, sell or rent) their "scrubbed" (*i.e.*, designed to be anonymous) health data. There are numerous startups that have built platforms to offer pay-to-access information to researchers from universities, medical institutes, and pharmaceutical companies – and that allow consumers such as Plaintiffs and class members to monetize their own PHI and turn a profit on it if they so choose.

95. Consumers who are customers of these startups receive compensation for allowing access to information such as that which was compromised in the Data Breach, only anonymized or scrubbed.[37] By way of the Data Breach, Luxottica has compromised not only Plaintiffs' and

[37] Depending on their health and demographics, users of CoverUS can generate the equivalent of $100 to $1,000 a month if they monetize their PHI. People with illnesses and special conditions that are of particular interest to researchers can earn even more money. Ben Schiller, *Can This App That Lets You Sell Your Health Data Cut Your Health Costs*, FAST CO. (Jan. 4, 2018), https://www.fastcompany.com/40512559/can-this-app-that-lets-you-sell-your-health-data-cut-your-health-costs.

class members' privacy, but also a substantial portion of the value of their PHI that is being misused and monetized by cyber-criminals.

96. The theft of PHI is harmful not only because of its lost value and the increased risk of identity theft it poses, but because of the direct risk posed to patient health. Cyberattacks and data breaches involving medical practices like Luxottica's are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

97. 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.[38]

98. 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.[39]

99. 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;

(d) Undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

---

[38] *See* Nsikan Akpan, *Ransomeware and date breaches linked to uptick in fatal heart attacks,* SCIENCE (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[39] *See* Sung J. Choi PhD, M. Eric Johnson PhD, Christoph U. Lehmann MD, *Data breach remediation efforts and their implications for hospital* quality, WILEY (Sept. 10, 2019), https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited Jan. 22, 2021).

(e) Losing patient medical history.[40]

100. Luxottica's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for patient and consumer privacy, and has exposed the PII and PHI of Plaintiffs and class members to cyber-criminals.

101. PII, including PHI, also has significant monetary value in part because criminals continue their efforts to obtain this data.[41] In other words, if any additional breach of sensitive data did not have incremental value to criminals, one would expect to see a reduction in criminal efforts to obtain such additional data over time. Instead, just the opposite has occurred. For example, the Identity Theft Resource Center reported 1,473 data breaches in 2019, which represents a 17 percent increase from the total number of breaches reported in 2018.[42]

102. The value of PII is key to unlocking many parts of the financial sector for consumers. Whether someone can obtain a mortgage, credit card, business loan, tax return, or even apply for a job depends on the integrity of their PII. Similarly, the businesses that request (or require) consumers to share their PII as part of a commercial transaction do so with the expectation that its integrity has not been compromised.

---

[40] *See, e.g.*, Lisa Vaas, *Ransomware attacks paralyze, and sometimes crush, hospitals*, NAKED SEC. (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/; Jessica Davis, *Data Breaches Will Cost Healthcare $4B in 2019, Threats Outpace Tech*, HEALTH IT SEC. (Nov. 5, 2019), https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech (last visited Jan. 22, 2021).

[41] George V. Hulme, *Data Breaches Rise as Cybercriminals Continue to Outwit IT*, CIO MAGAZINE (Sept. 28, 2014), http://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html.

[42] *2019 End-of-Year Data Breach Report* (2019), IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited Jan. 22, 2021).

103. Luxottica recognizes the value of PII and PHI, as its possession and processing of PII and PHI allows it to advance its own commercial or economic interests. Luxottica annually receives for the business's commercial purposes or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers.

104. Annual monetary losses for victims of identity theft are in the billions of dollars. In 2017, fraudsters stole $16.8 billion from consumers in the United States, which includes $5.1 billion stolen through bank account take-overs.[43]

105. The annual cost of identity theft is even higher. McAfee and the Center for Strategic and International Studies estimates that the likely annual cost to the global economy from cybercrime is $445 billion a year.[44]

106. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, in addition to the irreparable damage that may result from the theft of PII, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[45]

107. Even before the occurrence of identity theft, victims may spend valuable time and suffer from the emotional toll of a data breach.

---

[43] Al Pascual, Kyle Marchini, Sarah Miller, *2018 Identity fraud: Fraud Enters A New Era of Complexity*, JAVELIN (Feb. 6, 2018), https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity.

[44] *Facts + Statistics: Identity theft and cybercrime*, INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Jan. 22, 2021).

[45] Erika Harrell, Ph.D., *Victims of Identity Theft, 2014*, DOJ (Revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

108. Plaintiff Gervais has spent at least one hour responding to the Data Breach after receiving notice from Luxottica, including conducting independent online research regarding the scope of the breach and monitoring his credit score. He will continue to expend time reviewing account statements and any correspondence from insurers and healthcare providers to guard against medical fraud.

109. Plaintiffs Crockett and Rivera have each spent hours reading communications from Luxottica, reading information published about Luxottica that explains that Luxottica's severely delayed response was not sufficient and that Luxottica is downplaying the number of Social Security numbers compromised, and then by working through all of the PII and PHI data points that Luxottica might possess, such as Social Security number, address, credit card information, health savings account information, and email addresses, among others. Plaintiffs Crockett and Rivera will continue to spend time and resources reviewing bank statements, HSA statements, and ongoing notices from insurers and healthcare providers to try to protect themselves against medical fraud.

110. Plaintiff Doyle has spent at least one hour responding to the Data Breach after receiving notice from Luxottica, including discussing the impact of the Data Breach with his attorneys. He will continue to expend time reviewing account statements and his credit score when engaging in future credit transactions, and reviewing any correspondence from insurers and healthcare providers to guard against medical fraud.

111. Plaintiff Gloss has spent approximately four hours examining his bank statements and credit accounts to ensure that his PII and PHI had not already been used by a third party. Plaintiff Gloss also spent approximately two hours researching data privacy laws and requirements, and another two hours attempting to contact Cunningham Vision Care to request that they remove all of his PII and PHI from their database – though Cunningham Vision Care

indicated that it was unable to do so. Plaintiff Gloss will also continue to spend time and resources reviewing bank statements, credit transactions, and ongoing notices from insurers and healthcare providers to try to protect himself against future fraud.

112. The impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[46] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

113. In a recent survey conducted by the Medical Identity Fraud Alliance, a healthcare industry trade group, 52 percent of victims said their information was used to obtain government benefits like Medicare or Medicaid.[47] And 59 percent had their identity used to obtain healthcare, while 56 percent said a scammer parlayed their data into prescription drugs or medical equipment.[48] This is all the type of injury and harm, including actual fraud, Luxottica knows full well has been reported to it as being suffered by Plaintiffs and class members, and is directly traceable to the Data Breach. This harm is not merely just possible or certainly impending, it actually happened and is ongoing, and Plaintiffs and all class members are in imminent and immediate danger of being further subjected to this injury.

---

[46] *Identity Theft: The Aftermath 2017*, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited Jan. 22, 2021).

[47] Christopher Burgess, *Protect What You Collect: Keep Protected Health Information Secure*, SEC. INTELLIGENCE (Nov. 3, 2015), https://securityintelligence.com/protect-what-you-collect-keep-protected-health-information-secure/.

[48] *Id.*

114. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate/lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[49]

115. It is no wonder, then, that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey[50] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft; and
- 7% reported feeling suicidal.

116. There may also be a significant time lag between when PII and PHI is stolen and when it is actually misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

---

[49] *Id.*

[50] *Id.*

> [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.[51]

117. Thus, 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 Plaintiffs and class members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and class members must vigilantly monitor their financial and medical accounts for many years to come.

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

119. Plaintiffs and class members have been damaged by the compromise of their PII and PHI in the Data Breach.

120. Plaintiffs' PII and PHI were compromised and is now in the hands of data thieves as a direct and proximate result of the Data Breach.

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

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

---

[51] Report to Congressional Requesters, *PERSONAL INFORMATION, Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV'T ACCOUNTABILITY OFF. (June 2007), http://www.gao.gov/new.items/d07737.pdf.

123. As the result of the Data Breach, Plaintiffs and class members have suffered or will suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

(a) identity theft and fraud resulting from theft of their PII and PHI;

(b) costs associated with the detection and prevention of identity theft and unauthorized use of their online accounts, including financial accounts;

(c) losing the inherent value of their PII and PHI;

(d) costs associated with purchasing credit monitoring and identity theft protection services;

(e) unauthorized access to and misuse of their online accounts;

(f) unauthorized access to and misuse of their PHI;

(g) unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

(h) lowered credit scores resulting from credit inquiries following fraudulent activities;

(i) costs associated with time spent and the loss of productivity or enjoyment of one's life attempting to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, and addressing other varied instances of identity theft;

(j) the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII and PHI being in the possession of one or more unauthorized third parties; and

(k) continued risk of exposure to hackers and thieves of their PII and PHI, which remains in Luxottica's possession and is subject to further breaches so long as Luxottica fails to undertake appropriate and adequate measures to protect Plaintiffs and class members.

124. Additionally, Plaintiffs and class members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[52]

125. Indeed, Plaintiffs have taken steps to protect themselves from identity theft and fraud. For example, Plaintiff Gervais does not share PII or PHI through websites he knows to be unsecure and he periodically monitors his credit report (such reviewing of his credit score having increased in frequency following his receipt of notice of the Data Breach). Before the Data Breach, these measures were successful – Mr. Gervais had not previously suffered identity theft and, to his knowledge, had not been the victim of a data breach compromising his PHI.

126. Ms. Crocket had been actively rebuilding her credit before the Data Breach and was actively monitoring her credit report to ensure there was no negative activity, such as identity theft or someone misusing her credit to her detriment. Before the Data Breach, these actions had been successful and Ms. Crocket had not previously suffered identity theft, or, to her knowledge, been the victim of a data breach compromising her PHI or PII.

127. Mrs. Rivera has a history of monitoring her PII and PHI, including her bank cards. She is careful with the websites she visits and on which she shares PHI or PII. Before the Data

[52] Richard Turner, *Beyond the Bottom Line: The Real Cost of Data Breaches*, FIREEYE (May 11, 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html.

Breach, these efforts had been successful, and Mrs. Rivera had not previously suffered identity theft, or, to her knowledge, been the victim of a data breach compromising her PHI or PII.

128. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, companies like Luxottica would have no reason to tout their data security efforts to their actual and potential customers.

129. Had the victims of the Data Breach, including Plaintiffs, known the truth about Luxottica's data security practices – that Luxottica would not adequately protect and store their data – they would have demanded that their eye care center not store or process their PII and PHI through Luxottica's computer data and storage systems and would not have paid for, or would have paid less for, services and goods at retailers or providers using Luxottica's systems, including Target Optical, LensCrafters, and Pearle Vision.

130. Additionally, Plaintiffs and class members have an interest in ensuring that their PII and PHI, which is believed to remain in the possession of Luxottica, 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.

131. Further, as a result of Luxottica's conduct, Plaintiffs and class members are forced to live with the anxiety that their PII and PHI – 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.

132. As a direct and proximate result of Luxottica's actions and inactions, Plaintiffs and class members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased and imminent risk of fraud, criminal misuse of their PII and PHI, and are at a continuing

risk of identity theft for years to come as result of the Data Breach and Luxottica's deceptive and unconscionable conduct.

V. CLASS ACTION ALLEGATIONS

133. Pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiffs seek certification of the following class and subclasses:

> **National Class**: All residents of the United States of America whose PII or PHI was compromised in the Data Breach.
>
> **California Subclass**: All residents of California whose PII or PHI was compromised in the Data Breach.
>
> **Connecticut Subclass**: All residents of Connecticut whose PII or PHI was compromised in the Data Breach.
>
> **Florida Subclass**: All residents of Florida whose PII or PHI was compromised in the Data Breach.
>
> **Missouri Subclass**: All residents of Missouri whose PII or PHI was compromised in the Data Breach.
>
> **Ohio Subclass**: All residents of Ohio whose PII or PHI was compromised in the Data Breach.
>
> **Wisconsin Subclass**: All residents of Wisconsin whose PII or PHI was compromised in the Data Breach.

134. The National Class and Subclasses are collectively referred to herein as the "Class."

135. Excluded from the Class are employees and doctors of Luxottica eye care centers and retailers, Luxottica itself, any entity in which Luxottica has a controlling interest, and Luxottica's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officers presiding over this matter, members of their immediate family, members of their judicial staff, and any judge sitting in the presiding court system who may hear an appeal of any judgment entered.

136. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is

impractical. Luxottica has admitted that hundreds of thousands of Patients across the country were affected by the Data Breach.

137. **Commonality and Predominance. Fed. R. Civ. P. 23(a)(2) and (b)(3).** This action involves common questions of law and fact that predominate over any questions affecting individual class members. The common questions include, but are not limited to:

(a) Whether Luxottica knew or should have known that its computer and data storage systems were vulnerable to attack;

(b) Whether Luxottica omitted or misrepresented material facts regarding the security of its computer and data storage systems and their inability to protect vast amounts of sensitive data, including Plaintiffs' and class members' PII and PHI;

(c) Whether Luxottica failed to take adequate and reasonable measures to ensure such computer and data systems were protected;

(d) Whether Luxottica failed to take available steps to prevent and stop the Data Breach from happening;

(e) Whether Luxottica failed to disclose the material facts that it did not have adequate computer systems and security practices to safeguard PII and PHI;

(f) Whether Luxottica owed duties to Plaintiffs and class members to protect their PII and PHI;

(g) Whether Luxottica owed a duty to provide timely and accurate notice of the Data Breach to Plaintiffs and class members;

(h) Whether Luxottica breached its duties to protect the PII and PHI of Plaintiffs and class members by failing to provide adequate data security;

(i) Whether Luxottica breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and class members;

(j) Whether Luxottica's failure to secure Plaintiffs' and class members' PII and PHI in the manner alleged violated federal, state, and local laws and regulations, or industry standards;

(k) Whether Luxottica was negligent, reckless, or intentionally indifferent in its representations or omissions to Plaintiffs and class members concerning its security protocols;

(l) Whether Luxottica was negligent in making misrepresentations or omissions to Plaintiffs and class members;

(m) Whether Luxottica was negligent in establishing, implementing, and following security protocols;

(n) Whether the Plaintiffs' and class members' PII and PHI were compromised and exposed as a result of the Data Breach and the extent of that compromise and exposure;

(o) Whether Luxottica's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unauthorized access to, compromise, and/or theft of Plaintiffs' and class members' PII and PHI;

(p) Whether Luxottica's conduct amounted to violations of California consumer protection and data breach statutes;

(q) Whether Luxottica's conduct amounted to violations of Connecticut consumer protection and data breach statutes;

(r) Whether Luxottica's conduct amounted to violations of Florida consumer protection and data breach statutes;

(s) Whether Luxottica's conduct amounted to violations of Missouri consumer protection and data breach statutes;

(t) Whether Luxottica's conduct amounted to violations of Ohio consumer protection and data breach statutes;

(u) Whether Luxottica's conduct amounted to violations of Wisconsin consumer protection and data breach statutes;

(v) Whether, as a result of Luxottica's conduct, Plaintiffs and class members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled;

(w) Whether, as a result of Luxottica's conduct, Plaintiffs and class members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief;

(x) Whether Plaintiffs and class members are entitled to compensatory damages;

(y) Whether the Plaintiffs and class members are entitled to punitive damages; and

(z) Whether the Plaintiffs and class members are entitled to statutory damages.

138. **Typicality. Fed. R. Civ. P. 23(a)(3).** Plaintiffs' claims are typical of other class members' claims because Plaintiffs and class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

139. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class. Plaintiffs are members of the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation and consumer protection claims. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the interests of the Class.

140. **Risk of Inconsistent or Varying Adjudications. Fed. R. Civ. P. 23(b)(1).** As the proposed Class includes hundreds of thousands of Patients, there is significant risk of inconsistent

or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for Luxottica. For example, injunctive relief may be entered in multiple cases, but the ordered relief may vary, causing Luxottica to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which it will comply. Class action status is also warranted because prosecution of separate actions by the members of the Class would create a risk of adjudications with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

141. **Injunctive and Declaratory Relief. Fed. R. Civ. P. 23(b)(2).** Class certification is also appropriate under Rule 23(b)(2). Luxottica, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, Luxottica continues to maintain its inadequate security practices, retains possession of Plaintiffs' and the class members' PII and PHI, and has not been forced to change its practices or to relinquish PII and PHI by nature of other civil suits or government enforcement actions, thus making injunctive and declaratory relief a live issue and appropriate to the Class as a whole.

142. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual Plaintiffs and class members may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and class members are relatively small compared to the burden and expense required to individually litigate their claims against Luxottica,

and thus, individual litigation to redress Luxottica's wrongful conduct would be impracticable. Individual litigation by each class member would also strain the court system. Moreover, individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

143. Particular issues are appropriate for certification under **Fed. R. Civ. P. 23(c)(4)** because the claims present particular, common issues, the resolution of which would materially advance the resolution of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

(a) Whether class members' PII and PHI were accessed, compromised, or stolen in the Data Breach;

(b) Whether (and when) Luxottica knew about the Data Breach before it notified Plaintiffs and class members and whether Defendant failed to timely notify Plaintiffs and class members of the Data Breach;

(c) Whether Luxottica owed a legal duty to Plaintiffs and the Class;

(d) Whether Luxottica failed to take reasonable steps to safeguard the PII and PHI of Plaintiffs and class members;

(e) Whether Luxottica failed to adequately monitor its data security systems;

(f) Whether Luxottica's representations that they would secure and protect the PII and PHI of Plaintiffs and Class were facts that reasonable persons could be expected to rely upon when deciding whether to use Luxottica's services;

(g) Whether Luxottica misrepresented or omitted material information regarding the safety of their systems and services, specifically the security thereof, and Luxottica's ability to adequately safeguard Plaintiffs' and class members' PII and PHI;

(h) Whether Luxottica concealed material information about their inadequate data security measures from Plaintiffs and the Class;

(i) Whether Luxottica failed to comply with its applicable laws, regulations, and industry standards relating to data security;

(j) Whether Luxottica's acts, omissions, misrepresentations, and practices were likely to deceive consumers;

(k) Whether Luxottica knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class members' PII or PHI secure;

(l) Whether adherence to HIPAA regulations, FTC data security obligations, industry standard, and measures recommended by data security experts would have reasonably prevented the Data Breach.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE

Against Luxottica on Behalf of Plaintiffs and the National Class or, Alternatively, on Behalf of Plaintiff Gervais and the California Subclass, Plaintiff Doyle and the Connecticut Subclass, Plaintiff Payne on Behalf of M.P. and the Florida Subclass, Plaintiff Gloss and the Missouri Subclass, Plaintiff Rivera and the Ohio Subclass, and Plaintiff Crockett and the Wisconsin Subclass

144. Plaintiffs repeat the allegations in paragraphs 1 – 143 in this Complaint, as if fully alleged herein.

145. Luxottica required Plaintiffs and class members to submit non-public PII and PHI to obtain medical services.

146. Luxottica, in offering optometry and vision services to its customers and the ability to schedule appointments through the Scheduling Application, knew that Plaintiffs and class members' sensitive PII and PHI would be stored or processed by Luxottica computer and data storage systems, including on the Scheduling Application. Luxottica, in fact, stored and/or processed this PII through and on its computer systems and/or databases, utilizing the Scheduling Application.

147. By collecting, storing, and using this data, Luxottica had a duty of care to Plaintiffs and class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting this PII and PHI in Luxottica's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Luxottica's security systems and data storage architecture to ensure that Plaintiffs' and class members' PII and PHI were adequately secured and protected; (b) implementing processes that would detect an unauthorized breach of Luxottica's security systems and data storage architecture in a timely manner; (c) timely acting on all warnings and alerts, including public information, regarding Luxottica's security vulnerabilities and potential compromise of the PII and PHI of Plaintiffs and class members; (d) maintaining data security measures consistent with industry standards and applicable state and federal law and other requirements discussed herein; and (e) timely and adequately informing Plaintiffs and class members if and when a data breach occurred, notwithstanding undertaking (a) through (d) above.

148. Luxottica had common law duties to prevent foreseeable harm to Plaintiffs and class members. These duties existed because Plaintiffs and class members were the foreseeable and probable victims of any inadequate security practices in Luxottica's affirmative collection of Patients' PII and PHI. In fact, not only was it foreseeable that Plaintiffs and class members would be harmed by the failure to protect their PII and PHI because hackers routinely attempt to steal

such information and use it for nefarious purposes, Luxottica knew that it was more likely than not Plaintiffs and other class members would be harmed by such theft.

149. Luxottica had a duty to monitor, supervise, control, or otherwise provide oversight to safeguard the PII that was collected, stored, and processed by Luxottica computer and data storage systems.

150. Luxottica's duties to use reasonable security measures also arose as a result of the special relationship that existed between Luxottica, on the one hand, and Plaintiffs and class members, on the other hand. The special relationship, which is recognized by laws and regulations including but not limited to HIPAA as well as common law, arose because Plaintiffs and class members entrusted Luxottica with their PII and PHI by virtue of their participation in the optometry and vision services offered by Luxottica. Luxottica alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

151. Luxottica's duty to use reasonable security measures under HIPAA required Luxottica to "reasonably protect" confidential data from "[a]ny 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).

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

153. Luxottica's duties to use reasonable data security measures also arose under Section 5 of the FTC 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 PII and PHI. Various FTC publications and data security breach orders further form the basis of Luxottica's duties. In addition, individual states have enacted statutes based

upon the FTC Act, including California's Unfair Competition Law, the Connecticut Unfair Trade Practices Act, the Florida Deceptive and Unfair Trade Practices Act, and the Missouri Merchandising Practices Act, that also created a duty.

154. Luxottica's duties to use reasonable data security measures also arose under the CCPA, which imposes a "duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."

155. Luxottica's duties to use reasonable data security measures also arose under the CCRA, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

156. Luxottica's duties to use reasonable data security measures also arose under the CMIA, which required Defendant to, among other things, protect and preserve the integrity of electronic medical information. *See* Cal. Civ. Code §§56.06, 56.101(a), 56.101(b)(1)(A).

157. The harm that has occurred is the type of harm the FTC Act (and similar state statutes, including those of California, Connecticut, Florida, Missouri, Ohio, and Wisconsin), and the CCPA, CCRA, and CMIA, were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of the businesses' failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and class members.

158. Luxottica knew or should have known that its computer systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII and PHI.

159. Luxottica knew or should have known that a breach of its systems and data storage architecture would inflict millions of dollars of damages upon Plaintiffs and class members, and Luxottica was therefore charged with a duty to adequately protect this critically sensitive information.

160. Luxottica breached the duties it owed to Plaintiffs and class members described above and thus, was negligent. The specific negligent acts and omissions committed by Luxottica include, but are not limited to, the following:

(a) Failing to adopt, implement, and maintain adequate security measures (including adequate security systems, protocols, and practices) to safeguard Plaintiffs' and class members' PII and PHI;

(b) Failing to adequately monitor the security of its networks and systems;

(c) Failing to periodically ensure that its Scheduling Application had plans in place to maintain reasonable data security safeguards;

(d) Allowing unauthorized access to Plaintiffs' and class members' PII and PHI;

(e) Failing to detect in a timely manner that Plaintiffs' and class members' PII and PHI had been compromised; and

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

161. Luxottica also failed to exercise reasonable care and breached the duties it owed Plaintiffs and class members when it provided the thieves and/or subsequent unauthorized recipients of the compromised information with additional time and cover to further purloin and re-sell the compromised PII and PHI belonging to Plaintiffs and the Class; provided the thieves

and the purchasers and/or other subsequent unauthorized recipients with an opportunity to directly defraud Plaintiffs and the Class; and failed to promptly notify Plaintiffs and class members of the fact that their PII and PHI were compromised and in imminent jeopardy of falling further into the hands of cyber criminals.

162. But for Luxottica's wrongful and negligent breach of its duties owed to Plaintiffs and class members, their PII and PHI would not have been compromised.

163. It was foreseeable that Luxottica's failure to use reasonable measures to protect Plaintiffs' and class members' PII and PHI would result in injury to Plaintiffs and class members.

164. Further, the Data Breach was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

165. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and class members' PII and PHI would result in one or more types of injuries to Plaintiffs and class members.

166. As a direct and proximate result of Luxottica's negligence, Plaintiffs and class members have been injured and are entitled to compensatory and consequential damages in an amount to be proven at trial. Such injuries include those described above, including one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the compromised PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Luxottica, reviewing bank statements, payment card statements, provider and insurance statements, and credit reports; expenses and time spent

initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII and PHI; and other economic and non-economic harm.

167. Plaintiffs and class members are also entitled to injunctive relief requiring Luxottica to, among other things: (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) provide adequate credit monitoring and identity theft protection services to Plaintiffs and all class members.

COUNT II
NEGLIGENCE PER SE

Against Luxottica on Behalf of Plaintiffs and the National Class or, Alternatively, on Behalf of Plaintiff Doyle and the Connecticut Subclass, Plaintiff Payne on Behalf of M.P. and the Florida Subclass, Plaintiff Gloss and the Missouri Subclass, Plaintiff Rivera and the Ohio Subclass, and Plaintiff Crockett and the Wisconsin Subclass

168. Plaintiffs repeat the allegations in paragraphs 1 – 143 in this Complaint, as if fully alleged herein, and assert this claim in the alternative to their negligence claim to the extent necessary.

169. Pursuant to the FTC Act, 15 U.S.C. §45, Luxottica had a duty to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiffs and class members.

170. The FTC Act prohibits "unfair . . . practices in or affecting commerce," which the FTC has interpreted to include businesses' failure to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Luxottica's duty in this regard. In addition, individual states have enacted statutes based upon the FTC Act, including the UCL, the CUTPA, the FDUTPA, and the MMPA, that also created a duty.

171. Pursuant to HIPAA, Luxottica had a duty to implement reasonable safeguards to protect Plaintiffs' and class members' PII. *See* 42 U.S.C. §1302(d), *et seq.*

172. Pursuant to HIPAA, Luxottica 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.

173. Pursuant to the Gramm-Leach-Bliley Act, Luxottica had a duty to protect the security and confidentiality of Plaintiffs' and class members' PII. *See* 15 U.S.C. §6801.

174. Pursuant to the FCRA, Luxottica had a duty to adopt, implement, and maintain adequate procedures to protect the security and confidentiality of Plaintiffs' and class members' PII. *See* 15 U.S.C. §1681(b).

175. Luxottica's duties to use reasonable data security measures also arose under the CCPA, Cal. Civ. Code §1798.100, *et seq.*, which imposes a "duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."

176. Pursuant to the CMIA, Cal. Civ. Code §56, *et seq.*, Luxottica had a statutory duty to, among other things, protect and preserve the integrity of electronic medical information. *See* Cal. Civ. Code §§56.06, 56.101(a), 56.101(b)(1)(A).

177. Luxottica's duties to use reasonable data security measures also arose under the CCRA, Cal. Civ. Code §1798.80, *et seq.*, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

178. Pursuant to the UCL, Luxottica had duty to provide fair and adequate computer systems and data security to safeguard the PII and PHI of Plaintiffs and class members. *See* Cal. Bus. & Prof. Code §17200, *et seq.*

179. Pursuant to the CUTPA, Luxottica had duty to provide fair and adequate computer systems and data security to safeguard the PII and PHI of Plaintiffs and class members. *See* Conn. Gen. Stat. §42-110a, *et seq.*

180. Pursuant to the FDUTPA, Luxottica had duty to provide fair and adequate computer systems and data security to safeguard the PII and PHI of Plaintiffs and class members. *See* Fla. Stat. §501.201, *et seq.*

181. Pursuant to the MMPA, Luxottica had duty to provide fair and adequate computer systems and data security to safeguard the PII and PHI of Plaintiffs and class members. *See* Mo. Stat. §407.020(1), *et seq.*

182. Luxottica solicited, gathered, and stored PII and PHI of Plaintiffs and the class members to facilitate transactions which affect commerce.

183. Luxottica violated the FTC Act (and similar state statutes), the CCPA, CCRA, CMIA, HIPAA, the FCRA, and the Graham-Leach-Bliley Act by failing to use reasonable measures to protect PII and PHI of Plaintiffs and class members and not complying with applicable industry standards, as described herein. Luxottica's conduct was particularly unreasonable given the nature and amount of PII and PHI obtained and stored and the foreseeable consequences of a data breach on Luxottica's systems.

184. Luxottica's violation of the FTC Act (and similar state statutes) as well as its violations of the CCPA, CMIA, CCRA, HIPAA, the FCRA, and the Graham-Leach-Bliley Act constitute negligence *per se*.

185. Plaintiffs and the class members are within the class of persons that the FTC Act (and similar state statutes), HIPAA, the FCRA, and the Graham-Leach-Bliley Act were intended to protect. Plaintiff Gervais and the California Subclass members are within the class of persons that the CCPA, CMIA, and CCRA were intended to protect.

186. The harm that occurred as a result of the breach is the type of harm the FTC Act (and similar state statutes), as well as the CCPA, CMIA, CCRA, HIPAA, the FCRA, and the Graham-Leach-Bliley Act were 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 caused the same harm as that suffered by Plaintiffs and the class members.

187. As a direct and proximate result of Luxottica's negligence *per se*, Plaintiffs and class members have suffered, and continue to suffer, damages arising from the breach as described herein and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

188. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the compromised PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Luxottica, reviewing bank statements, payment card statements, provider and insurance statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII and PHI; and other economic and non-economic harm.

COUNT III
DECLARATORY JUDGMENT

Against Luxottica on Behalf of Plaintiffs and the National Class or, Alternatively, on Behalf of Plaintiff Gervais and the California Subclass, Plaintiff Doyle and the Connecticut Subclass, Plaintiff Payne on Behalf of M.P. and the Florida Subclass, Plaintiff Gloss and the Missouri Subclass, Plaintiff Rivera and the Ohio Subclass, and Plaintiff Crockett and the Wisconsin Subclass

189. Plaintiffs repeat the allegations in paragraphs 1 – 143 in this Complaint, as if fully alleged herein.

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

191. An actual controversy has arisen in the wake of the Data Breach regarding Luxottica's present and prospective common law and other duties to reasonably safeguard its users' PII, and whether Luxottica is currently maintaining data security measures adequate to protect Plaintiffs and class members from further data breaches that compromise their PII and PHI. Plaintiffs and class members remain at imminent risk that further compromises of their PII and PHI will occur in the future. This is true even if they are not actively using Luxottica's products or services.

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

(a) Luxottica continues to owe a legal duty to secure users' PII and PHI and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

(b) Luxottica continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiffs and class members' PII and PHI.

193. The Court also should issue corresponding prospective injunctive relief pursuant to 28 U.S.C. §2202, requiring Luxottica to employ adequate security practices consistent with law and industry standards to protect its users' PII and PHI.

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

195. The hardship to Plaintiffs and class members if an injunction does not issue exceeds the hardship to Luxottica if an injunction is issued. Among other things, if another data breach occurs at Luxottica, Plaintiffs and class members will likely be subjected to fraud, identity theft, and other harms described herein. On the other hand, the cost to Luxottica of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Luxottica has a pre-existing legal obligation to employ such measures.

196. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Luxottica, thus eliminating additional injuries that would result to Plaintiffs, class members, and the millions of other Luxottica customers whose PII and PHI would be further compromised.

COUNT IV
BREACH OF CONFIDENCE

Against Luxottica on Behalf of Plaintiffs and the National Class or, Alternatively, on Behalf of Plaintiff Gervais and the California Subclass, Plaintiff Doyle and the Connecticut Subclass, Plaintiff Payne on Behalf of M.P. and the Florida Subclass, Plaintiff Gloss and the Missouri Subclass, Plaintiff Rivera and the Ohio Subclass, and Plaintiff Crockett and the Wisconsin Subclass

197. Plaintiffs repeat the allegations in paragraphs 1 – 143 in this Complaint, as if fully alleged herein.

198. At all times during Plaintiffs' and class members' interactions with Luxottica, Luxottica was fully aware of the confidential and sensitive nature of Plaintiffs' and class members' PII and PHI.

199. Luxottica's relationship with Plaintiffs and class members was governed by terms and expectations that Plaintiffs' and class members' PII and PHI would be collected, stored, and protected in confidence, and would not be disclosed to the public or any unauthorized third parties.

200. Plaintiffs and class members provided their respective PII and PHI, which were both confidential and novel, to Luxottica with the explicit and implicit understandings that Luxottica would protect and not permit their PII and PHI to be disseminated to the public or any unauthorized parties.

201. Plaintiffs and class members also provided their respective PII and PHI to Luxottica with the explicit and implicit understandings that Luxottica would take precautions to protect the PII and PHI from unauthorized disclosure, such as following basic principles of encryption and information security practices.

202. Luxottica voluntarily received in confidence Plaintiffs' and class members' PII and PHI with the understanding that PII and PHI were confidential and novel and, as such, would not be disclosed or disseminated to the public or any unauthorized third parties.

203. Due to Luxottica's failure to prevent, detect, and avoid the Data Breach from occurring by following best information security practices to secure Plaintiffs' and class members' PII and PHI, Luxottica caused Plaintiffs' and class members' PII and PHI to be disclosed and misappropriated to the public and unauthorized third parties beyond Plaintiffs' and class members' confidence, and without their express permission.

204. But for Luxottica's disclosure of Plaintiffs' and class members' PII and PHI in violation of the parties' understanding of confidence, their PII and PHI would not have been compromised, stolen, viewed, accessed, and/or used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiffs' and class members' PII and PHI, as well as the resulting damages.

205. The injury and harm Plaintiffs and class members suffered was the reasonably foreseeable result of Luxottica's unauthorized disclosure of Plaintiffs' and class members' PII and PHI. Luxottica knew its computer systems and technologies for accepting, securing, and storing Plaintiffs' and class members' PII and PHI had serious security vulnerabilities because Luxottica failed to observe even basic information security practices or correct known security vulnerabilities.

206. As a direct and proximate result of Luxottica's breaches of confidence, Plaintiffs and class members have been injured and were damaged as discussed herein and as will be proven at trial.

207. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the compromised PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses

and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Luxottica, reviewing bank statements, payment card statements, provider and insurance statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII and PHI; and other economic and non-economic harm.

COUNT V
UNJUST ENRICHMENT

Against Luxottica on Behalf of Plaintiffs and the National Class or, Alternatively, on Behalf of Plaintiff Gervais and the California Subclass, Plaintiff Doyle and the Connecticut Subclass, Plaintiff Payne on Behalf of M.P. and the Florida Subclass, Plaintiff Gloss and the Missouri Subclass, Plaintiff Rivera and the Ohio Subclass, and Plaintiff Crockett and the Wisconsin Subclass

208. Plaintiffs repeat the allegations in paragraphs 1 – 143 in this Complaint, as if fully alleged herein.

209. Plaintiffs and class members conferred a monetary benefit on Luxottica in the form of monies or fees paid for services or goods from Luxottica. Luxottica had knowledge of this benefit when it accepted the money from Plaintiffs and class members.

210. The monies or fees paid by Plaintiffs and class members were supposed to be used by Luxottica, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiffs and class members.

211. Luxottica failed to provide reasonable security, safeguards, and protections to the PII and PHI of Plaintiffs and class members, and as a result Plaintiffs and class members overpaid Luxottica as part of services they purchased.

212. Luxottica failed to disclose to Plaintiffs and class members that its computer systems and security practices were inadequate to safeguard users' and former users' PII and PHI against theft.

213. Under principles of equity and good conscience, Luxottica should not be permitted to retain the money belonging to Plaintiffs and class members because Luxottica failed to provide adequate safeguards and security measures to protect Plaintiffs' and class members' PII, including PHI, that they paid for but did not receive.

214. Luxottica wrongfully accepted and retained these benefits to the detriment of Plaintiffs and class members.

215. Luxottica's enrichment at the expense of Plaintiffs and class members is and was unjust. As a result of Luxottica's wrongful conduct, as alleged above, Plaintiffs and class members are entitled under the unjust enrichment laws of all 50 states to restitution and disgorgement of all profits, benefits, and other compensation obtained by Luxottica, plus attorneys' fees, costs, and interest thereon.

COUNT VI
BREACH OF FIDUCIARY DUTY

Against Luxottica on Behalf of Plaintiffs and the National Class or, Alternatively, on Behalf of Plaintiff Gervais and the California Subclass, Plaintiff Doyle and the Connecticut Subclass, Plaintiff Payne on Behalf of M.P. and the Florida Subclass, Plaintiff Gloss and the Missouri Subclass, Plaintiff Rivera and the Ohio Subclass, and Plaintiff Crockett and the Wisconsin Subclass

216. Plaintiffs repeat the allegations in paragraphs 1 – 143 in this Complaint, as if fully alleged herein.

217. In light of the special relationship between Luxottica and Plaintiffs and class members, whereby Luxottica became guardians of Plaintiffs' and class members' PII and PHI, Luxottica became a fiduciary by its undertaking and guardianship of the PII and PHI, to act primarily for the benefit of its patients, including Plaintiffs and class members: (a) for the safeguarding of Plaintiffs' and class members' PII and PHI; (b) to timely notify Plaintiffs and class members of a data breach and disclosure; and (c) maintain complete and accurate records of what patient information (and where) Luxottica did and does store.

218. Luxottica has a fiduciary duty to act for the benefit of Plaintiffs and class members upon matters within the scope of its patients' relationship, in particular, to keep secure the PII and PHI of its patients.

219. Luxottica breached its fiduciary duties to Plaintiffs and class members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and class members' PII and PHI.

220. Luxottica breached its fiduciary duties owed to Plaintiffs and class members by failing to timely notify or warn Plaintiffs and class members of the Data Breach.

221. Luxottica breached its fiduciary duties owed to Plaintiffs and class members by failing to ensure the confidentiality and integrity of electronic PHI that Luxottica created, received, maintained, and transmitted, in violation of 45 C.F.R. §164.306(a)(1).

222. Luxottica breached its fiduciary duties owed to Plaintiffs and 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).

223. Luxottica breached its fiduciary duties owed to Plaintiffs and 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).

224. Luxottica breached its fiduciary duties owed to Plaintiffs and 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).

225. Luxottica breached its fiduciary duties owed to Plaintiffs and 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).

226. Luxottica breached its fiduciary duties owed to Plaintiffs and 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).

227. Luxottica breached its fiduciary duties owed to Plaintiffs and 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).

228. Luxottica breached its fiduciary duties owed to Plaintiffs and 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. §164.602, *et seq*.

229. Luxottica breached its fiduciary duties owed to Plaintiffs and 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 164.308(a)(5).

230. Luxottica breached its fiduciary duties owed to Plaintiffs and 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).

231. Luxottica breached its fiduciary duties to Plaintiffs and class members by otherwise failing to safeguard Plaintiffs' and class members' PII and PHI.

232. As a direct and proximate result of Luxottica's breach of its fiduciary duties, Plaintiffs and class members have suffered and will suffer injury, including but not limited to: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the compromised PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Luxottica, reviewing bank statements, payment card statements, provider and insurance statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII and PHI; and other economic and non-economic harm.

233. As a direct and proximate result of Luxottica's breaches of its fiduciary duties, Plaintiffs and class members have suffered and will continue to suffer other forms of injury or harm, and other economic and non-economic losses.

COUNT VII
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT
15 U.S.C. §1681 et seq.

Against Luxottica on Behalf of Plaintiffs and the National Class or, Alternatively, on Behalf of Plaintiff Gervais and the California Subclass, Plaintiff Doyle and the Connecticut Subclass, Plaintiff Payne on Behalf of M.P. and the Florida Subclass, Plaintiff Gloss and the Missouri Subclass, Plaintiff Rivera and the Ohio Subclass, and Plaintiff Crockett and the Wisconsin Subclass

234. Plaintiffs repeat the allegations in paragraphs 1 – 143 in this Complaint, as if fully alleged herein.

235. 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).

236. 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).

237. 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).

238. 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).

239. 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).

240. Plaintiffs' and class members' PII and PHI, in whole or in part, constitute "medical information" because it contains information that relates to the past, present, or future health of

Plaintiffs and class members, the provision of health care to Plaintiffs and class members, or the payment for the provision of health care to Plaintiffs and class members.

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

242. Plaintiffs' and class members' PII and PHI constitute a "consumer report" because the information bears on their character, reputation, personal characteristics, or mode of living, and is used and collected by Defendant for, among other things, determining Plaintiffs' and class members' healthcare needs, determining the scope of and eligibility of Plaintiffs' and class members' health or vision insurance coverage, and payments for Plaintiffs' and class members' health care and eyewear purchases.

243. Luxottica is a "consumer reporting agency" because, on a cooperative nonprofit basis or for monetary fees, Luxottica 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. Among other actions, Luxottica regularly assembles and transmits consumer reports on its Patients, including Plaintiffs and class members, to third-party service providers for a fee (unrelated to the provision of healthcare services) so that those third-party service providers may use those consumer reports to determine the Patients' creditworthiness, both for Luxottica and for other parties.

244. As a Consumer Reporting Agency, Luxottica 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 Plaintiffs and class members' PII and PHI)

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. §1681(b).

245. Luxottica, however, willfully or recklessly violated the FCRA by failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and class members' PII and PHI 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 Plaintiffs and class members' PII and PHI;

(d) Failing to detect in a timely manner that Plaintiffs and class members' PII and PHI had been compromised; and

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

246. As a proximate result of Luxottica's intentional or reckless violation of the FCRA and the resulting Data Breach, Plaintiffs' and class members' PII and PHI were accessed by unauthorized third parties in the public domain.

247. As a proximate result of Luxottica's intentional or reckless violation of the FCRA and the resulting Data Breach, Plaintiffs and class members were – and continue to be – damaged by the compromise and disclosure of their PII and PHI, the loss of control of their PII and 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, lost value of the PII and PHI, and loss of privacy.

248. Plaintiffs and class members are therefore entitled to compensation for their actual damages including, among other things: (a) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (b) 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; (c) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; (d) anxiety and emotional distress; (e) statutory damages of not less than $100, and not more than $1,000, each; and (f) attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681n(a).

COUNT VIII
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT
15 U.S.C. §1681 et seq.

Against Luxottica on Behalf of Plaintiffs and the National Class or, Alternatively, on Behalf of Plaintiff Gervais and the California Subclass, Plaintiff Doyle and the Connecticut Subclass, Plaintiff Payne on Behalf of M.P. and the Florida Subclass, Plaintiff Gloss and the Missouri Subclass, Plaintiff Rivera and the Ohio Subclass, and Plaintiff Crockett and the Wisconsin Subclass

249. Plaintiffs repeat the allegations in paragraphs 1 – 143 in this Complaint, as if fully alleged herein.

250. 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).

251. 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).

252. 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).

253. 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).

254. 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).

255. Plaintiffs' and class members' PII and PHI, in whole or in part, constitute "medical information" because it contains information that relates to the past, present, or future health of Plaintiffs and class members, the provision of health care to Plaintiffs and class members; or the payment for the provision of health care to Plaintiffs and class members.

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

257. Plaintiffs' and the class members' PII and PHI constitute a "consumer report" because the information bears on their character, reputation, personal characteristics, or mode of living, and is used and collected by Luxottica for, among other things, determining Plaintiffs' and class members' healthcare needs, determining the scope of and eligibility of Plaintiffs' and class members' health or vision insurance coverage, and payments for Plaintiffs' and class members' health care and eyewear purchases.

258. Luxottica is a "consumer reporting agency" because, on a cooperative nonprofit basis or for monetary fees, Luxottica 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. Among other actions, Luxottica regularly assembles and transmits consumer reports on its Patients, including Plaintiffs and class members, to third-party service providers for a fee (unrelated to the provision of healthcare services) so that those third-party service providers may use those consumer reports to determine the Patients' creditworthiness, both for Luxottica and for other parties.

259. As a Consumer Reporting Agency, Luxottica 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 Plaintiffs' and class members' PII and PHI) 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).

260. Luxottica, however, negligently violated the FCRA by failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and class members' PII and PHI 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 Plaintiffs' and class members' PII and PHI;

(d) Failing to detect in a timely manner that Plaintiffs' and class members' PII and PHI had been compromised; and

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

261. As a proximate result of Luxottica's negligent violation of the FCRA and the resulting Data Breach, Plaintiffs and class members' PII and PHI were accessed and compromised by unauthorized third parties in the public domain.

262. As a proximate result of Luxottica's negligent violation of the FCRA and the resulting Data Breach, Plaintiffs and class members were – and continue to be – damaged by the compromise and disclosure of their PII and PHI, the loss of control of their PII and 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, the lost value of their PHI and PII, and loss of privacy.

263. Plaintiffs and class members are therefore entitled to compensation for their actual damages including, among other things: (a) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (b) 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; (c) deprivation of the value of their PII and PHI, for which

there is a well-established national and international market; (d) anxiety and emotional distress; and (e) attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681n(a).

COUNT IX
CALIFORNIA'S UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code §17200, et seq.

Against Luxottica on Behalf of Plaintiff Gervais and the California Subclass

264. Plaintiff Gervais (for the purpose of this section, "Plaintiff"), repeats the allegations in paragraphs 1 – 143 in this Complaint, as if fully alleged herein.

265. Luxottica is a "person" as defined by Cal. Bus. & Prof. Code §17201.

266. Luxottica violated Cal. Bus. & Prof. Code §17200, *et seq.*by engaging in unlawful, unfair, and deceptive business acts and practices.

267. Luxottica's unfair acts and practices include:

(a) Luxottica failed to implement and maintain reasonable security measures to protect Plaintiff's and California Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Luxottica failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents in the healthcare sector. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and California Subclass members whose PII has been compromised;

(b) Luxottica's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. §45, the CCRA, Cal. Civ. Code §1798.81.5 *et seq.*, and the CCPA, Cal. Civ. Code §1798.100, *et seq.*;

(c) Luxottica's failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any

countervailing benefits to consumers or competition. Moreover, because consumers could not know of Luxottica's inadequate security, consumers could not have reasonably avoided the harms that Luxottica caused; and

(d) Engaging in unlawful business practices by violating Cal. Civ. Code §1798.82.

268. Luxottica has engaged in "unlawful" business practices by violating multiple laws, including the CCRA, Cal. Civ. Code §1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §1780, *et seq.*, the FTC Act, 15 U.S.C. §45, the CCPA, Cal. Civ. Code §1798.100, *et seq.*, and California common law.

269. Luxottica's unlawful, unfair, and deceptive acts and practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass members' PII, which was a direct and proximate cause of the Data Breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the healthcare sector, which was a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. §45, the CCRA, Cal. Civ. Code §1798.80, *et seq.*, and the CCPA, Cal. Civ. Code §1798.100 *et seq.*, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California Subclass members' PII and PHI, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. §45, and CCRA, Cal. Civ. Code §1798.80, *et seq.*; CMIA, Cal. Civ. Code §56, *et seq.*, and CCPA, Cal. Civ. Code §1798.100 *et seq.*

(f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California Subclass members' PII and PHI; and

(g) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. §45; CCRA, Cal. Civ. Code §1798.80, *et seq.*; CMIA, Cal. Civ. Code §56, *et seq*, and CCPA, Cal. Civ. Code §1798.100, *et seq.*

270. Luxottica's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Luxottica's data security and ability to protect the confidentiality of consumers' PII and PHI.

271. Luxottica intended to mislead Plaintiff and California Subclass members and induce them to rely on its misrepresentations and omissions.

272. Had Luxottica disclosed to Plaintiff and California Subclass members that its computer and data storage systems were not secure and, thus, vulnerable to attack, Luxottica would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Luxottica received, maintained, and compiled Plaintiff's and California Subclass members' PII and PHI, as part of the services Luxottica

provided and for which Plaintiff and California Subclass members paid, without advising Plaintiff and California Subclass members that Luxottica's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and California Subclass members' PII and PHI. Accordingly, Plaintiff and California Subclass members acted reasonably in relying on Luxottica's misrepresentations and omissions, the truth of which they could not have discovered.

273. Luxottica acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California Subclass members' rights. Past breaches within the healthcare industry put Luxottica on notice that its security and privacy protections were inadequate.

274. As a direct and proximate result of Luxottica's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages as described herein and as will be proved at trial. Absent Luxottica's unfair, unlawful, and fraudulent conduct, Plaintiffs and California Subclass members would have behaved differently and would not have purchased products or services from Luxottica or would have paid less for them. These losses also include the diminished value of Plaintiff's and California Subclass members' PII and PHI. Because the integrity of Plaintiff's and California Subclass members' PII and PHI is crucial to their future ability to engage in many aspects of commerce, including obtaining a mortgage, credit card, business loan, tax return, or even applying for a job, the diminishment of the integrity of that PII and PHI corresponds to a diminishment in value. In other words, Plaintiff and California Subclass members have both a present or future property interest diminished as a result of Luxottica's unfair, unlawful, and fraudulent acts and practices.

275. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Luxottica's unfair,

unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure §1021.5; injunctive relief; and other appropriate equitable relief.

COUNT X
CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code §1798.80, et seq.

Against Luxottica on Behalf of Plaintiff Gervais and the California Subclass

276. Plaintiff Gervais (for the purpose of this section, "Plaintiff"), repeats the allegations in paragraphs 1 – 143 in this Complaint, as if fully alleged herein.

277. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code §1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

278. Luxottica is a business that maintains Personal Information, within the meaning of Cal. Civ. Code §1798.81.5, about Plaintiff and California Subclass members.

279. Businesses that maintain computerized data that includes Personal Information are required to "notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code §1798.82(b). Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code §1798.82.

280. Luxottica is a business that maintains computerized data that includes Personal Information as defined by Cal. Civ. Code §1798.80.

281. Plaintiff and California Subclass members' Personal Information includes Personal Information as covered by Cal. Civ. Code §1798.82.

282. Because Luxottica reasonably believed that Plaintiff's and California Subclass members' PII, including PHI, was acquired by unauthorized persons during the Data Breach, Luxottica had an obligation to disclose the Data Breach immediately following its discovery to the owners or licensees of the PII and PHI (*i.e.*, Plaintiff and the California Subclass), as mandated by Cal. Civ. Code §1798.82. Indeed, Luxottica's own HIPAA Notice states that it would provide affected individuals with notice of a data breach regarding PHI.

283. By failing to disclose the Data Breach immediately following its discovery, Luxottica violated Cal. Civ. Code §1798.82.

284. As a direct and proximate result of Luxottica's violations of the Cal. Civ. Code §1798.81.5 and 1798.82, Plaintiff and California Subclass members suffered damages, as described above and as will be proven at trial.

285. Plaintiff and California Subclass members seek relief under Cal. Civ. Code §1798.84, including actual damages and injunctive relief.

COUNT XI
CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code §1798.100 et seq.

Against Luxottica on Behalf of Plaintiff Gervais and the California Subclass

286. Plaintiff Gervais (for the purpose of this section, "Plaintiff"), repeats the allegations in paragraphs 1 – 143 in this Complaint, as if fully alleged herein.

287. Plaintiff and California Subclass members are "consumer[s]" as that term is defined in Cal. Civ. Code. §1798.140(g).

288. Luxottica is a "business" as that term is defined in Cal. Civ. Code. §1798.140(c). As set forth above, Luxottica is a corporation organized or operated for the profit or financial benefit of its shareholders or other owners. Luxottica does business in the State of California.

Luxottica collects consumers' (including Plaintiff's and California Subclass members') personal information and determines the purposes and means of the processing of this personal information (*e.g.*, it designs the systems that process and store consumers' personal information). Luxottica has annual gross revenues in excess of twenty-five million dollars. Luxottica annually receives for the business's commercial purposes or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers.

289. Plaintiff's and California Subclass members' PII is "nonencrypted and nonredacted personal information" as that term is used in Cal. Civ. Code §1798.150(a)(1). At a minimum, this PII included the individual's first name or first initial and last name, in combination with medical information and health insurance information. In some instances, the PII also included Social Security numbers, financial information, and unique identification numbers issued on government documents (*e.g.*, driver's license numbers).

290. The Data Breach constitutes "an unauthorized access and exfiltration, theft, or disclosure" pursuant to Cal. Civ. Code §1798.150(a)(1).

291. Luxottica had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the Plaintiff's and California Subclass members' PII to protect said PII.

292. Luxottica breached the duty it owed to Plaintiff and California Subclass members described above. Luxottica breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and California Subclass members; (b) detect the breach while it was ongoing; and (c) maintain security systems consistent with industry standards.

293. Luxottica's breach of the duty it owed to Plaintiff and California Subclass members described above was the direct and proximate cause of the Data Breach. As a result, Plaintiff and California Subclass members suffered damages, as described above and as will be proven at trial.

294. Plaintiff seeks injunctive relief in the form of an order enjoining Luxottica from continuing the practices that constituted its breach of the duty owed to Plaintiff and California Subclass members as described above.

295. Plaintiff Gervais served Luxottica with a notice of claim under the CCPA on December 7, 2020, pursuant to Cal. Civ. Code. §1798.150(b). As of the filing date of this Consolidated Complaint, Plaintiff Gervais has received no satisfactory response from Luxottica. And as such, he seeks the full amount of available statutory damages on behalf of himself and the California Subclass.

COUNT XII
CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT
Cal. Civ. Code §56, et seq.

Against Luxottica on Behalf of Plaintiff Gervais and the California Subclass

296. Plaintiff Gervais (for the purpose of this section, "Plaintiff"), repeats the allegations in paragraphs 1 – 143 in this Complaint, as if fully alleged herein.

297. Luxottica is a "contractor," as defined in Cal. Civ. Code §56.05(d), a "pharmaceutical company," as defined in *id.* §56.05(1), and "a provider of health care," as defined in *id.* §56.06, and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

298. Luxottica is a person licensed under California under California's Business and Professions Code, Division 2. *See* Cal. Bus. Prof. Code §4000, *et seq.* Luxottica therefore qualifies as a "provider of health care" under the CMIA.

299. Plaintiff and the California Subclass are "patients" as defined in CMIA, Cal. Civ. Code §56.05(k) ("'Patient' means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains.").

300. Luxottica disclosed "medical information," as defined in CMIA, Cal. Civ. Code §56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code §56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Luxottica's employees, which allowed the hackers to see and obtain Plaintiff's and the California Subclass members' medical information.

301. Luxottica's negligence resulted in the release of individually identifiable medical information pertaining to Plaintiff and the California Subclass to unauthorized persons and the breach of the confidentiality of that information. Luxottica's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and California Subclass members' medical information in a manner that preserved the confidentiality of the information contained therein, in violation of Cal. Civ. Code §§56.06 and 56.101(a).

302. Luxottica's computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code §56.101(b)(1)(A).

303. Plaintiff and the California Subclass were injured and have suffered damages, as described above, from Luxottica's illegal disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§56.10 and 56.101, and therefore seek relief under Civ. Code §§56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorneys' fees, expenses and costs.

COUNT XIII
CONNECTICUT UNFAIR TRADE PRACTICES ACT
Conn. Gen. Stat. §42-110a et seq.

Against Luxottica on Behalf of Plaintiff Doyle and the Connecticut Subclass

304. Plaintiff Doyle (for the purpose of this section, "Plaintiff"), repeats the allegations in paragraphs 1 –143 in this Complaint, as if fully alleged herein.

305. The CUTPA, Conn. Gen. Stat. §42-110a *et seq.*, prohibits unfair methods of competition and unfair practices in the conduct of trade or commerce.

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

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

308. The CUTPA expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the FTC Act. *See* Conn. Gen. Stat. §42-110b(b).

309. Luxottica engaged in unfair business practices in violation of the CUTPA by, among other things, failing to implement and maintain reasonable security measures to protect its customers' PII and PHI, particularly in light of the heightened protections of PII and PHI mandated by HIPAA.

310. Specifically, Luxottica committed unfair or deceptive acts and practices by:

(a) Failing to maintain adequate computer systems and data security practices to safeguard PII and PHI;

(b) Failing to disclose that its computer systems and data security practices were inadequate to safeguard PII and PHI from theft;

(c) Continued gathering and storage of PII and PHI after Luxottica knew or should have known of the security vulnerabilities of its computer systems that were exploited in the Data Breach;

(d) Deceptively misrepresenting or omitting the true nature and character of Luxottica's data security practices and the privacy and security of PII and PHI of Plaintiff and Connecticut Subclass members, and;

(e) Continued gathering and storage of PII and PHI after Luxottica knew or should have known of the cyberattack and Data Breach and before Luxottica allegedly remediated the data security incident.

311. These unfair acts and practices violated duties imposed by laws, including but not limited to, the FTC Act, HIPAA, the FCRA, the Gramm- Leach-Bliley Act, and the CUTPA.

312. Luxottica's conduct offends public policy as established by, among other things, the FTC 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.

313. Luxottica's conduct caused substantial injury to Plaintiff and members of the Connecticut Subclass.

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

315. Plaintiff and members of the Connecticut Subclass reasonably expected Luxottica 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.

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

317. 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 Luxottica's data security practices; (b) Plaintiff and Connecticut Subclass members would not have entrusted their PII and PHI to Luxottica in the absence of promises that Luxottica would keep their information reasonably secure; and (c) Plaintiff and Connecticut Subclass members would not have entrusted their PII and PHI to Luxottica in the absence of the promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

318. As a direct and natural consequence of the violation of the CUTPA, Plaintiff and Connecticut Subclass members suffered injury and all other damages including, but not limited to: (a) the compromise, publication, or theft of their PII and PHI; (b) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft or unauthorized use of their PII and PHI; (c) 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; (d) the continued risk to their PII and PHI, which remains in Luxottica's possession and is subject to further unauthorized disclosures so long as Luxottica fails to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession; (e) 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 (f) the diminished value of their PII and PHI.

COUNT XIV
FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
Fla. Stat. §501.201, *et seq.*

Against Luxottica by Plaintiff Payne on Behalf of M.P. and the Florida Subclass

319. Plaintiff Payne on behalf of M.P. (for the purpose of this section, "Plaintiff"), repeats the allegations in paragraphs 1 – 143 in this Complaint, as if fully alleged herein.

320. The FDUTPA prohibits "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce . . ." Fla. Stat. §501.204(1).

321. Luxottica advertised, offered, or sold goods and services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

322. Luxottica engaged in unfair, unconscionable acts or practices, and unfair or deceptive practices in the conduct of trade and commerce in violation of Fla. Stat. §501.204(1), including by:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Florida Subclass members' PII and PHI, which was a direct and proximate cause of the Data Breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures knowing of the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Florida Subclass members' PII an PHI, including duties imposed by the FTC Act, 15 U.S.C. §45, and Florida's data security statute, Fla. Stat. §501.171(2), which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that Luxottica would protect the privacy and confidentiality of Plaintiff's and Florida Subclass members' PII and PHI, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that Luxottica would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Florida Subclass members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. §45, and Florida's data security statute, Fla. Stat. §501.171(2), which was a direct and proximate cause of the Data Breach;

(f) Omitting, suppressing, and concealing the material fact that Luxottica did not reasonable and adequately secure Plaintiff's and Florida Subclass members' PII and PHI; and

(g) Omitting, suppressing, and concealing the material fact that Luxottica did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Florida Subclass members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. §45, and Florida's data security statute, Fla. Stat. §501.171(2).

323. Luxottica's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Luxottica's data security and ability to protect the confidentiality of consumers' PII and PHI.

324. Had Luxottica disclosed to Plaintiff and Florida Subclass members that Luxottica's data systems were not secure and, thus, vulnerable to attack, Luxottica would have been forced to adopt reasonable data security measures and comply with the law. Instead, Luxottica received, maintained, and compiled Plaintiff's and Florida Subclass members' PII and PHI as part of the services Luxottica provided and for which Plaintiff and Florida Subclass members paid without advising them that Luxottica's data security measures were insufficient to maintain the safety and confidentiality of Plaintiff's and Florida Subclass members' PII and PHI. Accordingly, Plaintiff

and Florida Subclass members acted reasonably in relying on Luxottica's misrepresentations and omissions, the truth of which they could not have discovered.

325. As a direct and proximate result of Luxottica's unconscionable, unfair, and deceptive acts and practices, Plaintiff and Florida Subclass members have suffered and will continue to suffer injury, ascertainable losses of money and property, and monetary and non-monetary damages; loss of value of their PII and PHI; and an increased risk of fraud and identity theft.

326. Plaintiff and Florida subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. §501.211; declaratory and injunctive relief; reasonable attorney's fees and costs under Fla. Stat. §501.2105(1); and any other relief that is just and proper.

COUNT XV
MISSOURI MERCHANDISING PRACTICES ACT
Mo. Stat. §407.020(1), *et seq.*

Against Luxottica on Behalf of Plaintiff Gloss and the Missouri Subclass

327. Plaintiff Gloss (for the purpose of this section, "Plaintiff"), repeats the allegations in paragraphs 1 – 143 in this Complaint, as if fully alleged herein.

328. The MMPA provides:

> The act, … by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce . . . is defined to be an unlawful practice.

Mo. Stat. §407.020.

329. Plaintiff, the Missouri Subclass, and Luxottica are "persons" as defined in Mo. Stat. §407.020(1).

330. Luxottica advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Stat. §407.010(4), (6), and (7).

331. Plaintiff and the Missouri Subclass members purchased or leased goods or services primarily for personal, family, or household purposes.

332. By reasons of the conduct alleged herein, and by failing to provide reasonable security measure for the protection of PII and PHI of Plaintiff and Missouri Subclass members, Luxottica violated the provisions of the MPPA, Mo. Stat. §407.202.

333. Luxottica's actions as set forth above occurred in the conduct of trade or commerce.

334. Luxottica engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Stat. §407.020(1), including by:

(a) failing to maintain sufficient security to keep confidential and sensitive financial and personal information of Plaintiff and Missouri Subclass members from being hacked and compromised;

(b) misrepresenting or omitting material facts to the class, in connection with the sales of goods and providing services, by representing that Luxottica would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Missouri Subclass members' PII and PHI from authorized disclosure, release, data breaches, and theft;

(c) misrepresenting or omitting material facts to the class, in connection with the sale of goods and providing services, by representing that Luxottica did and would comply with the requirements of various federal and state laws pertaining to the privacy and security of Plaintiff's and Missouri Subclass members' personal information;

(d) failing to prevent the Data Breach and promptly notify consumers thereof, failing to maintain the privacy and security of Plaintiff's and Missouri Subclass members' personal information, in violation of duties imposed by and public policies reflected in the applicable federal and state laws; and

(e) engaging in deceptive, unfair, and unlawful acts or practices by failing to disclose the Data Breach to Plaintiff and Missouri Subclass members in a timely and accurate manner.

335. Due to the Data Breach, Plaintiff and the Missouri Subclass have lost property in the form of their PII and PHI and have suffered actual damages. Further, Luxottica's failure to adopt reasonable practices in protecting and safeguarding the confidential and sensitive PII and PHI of its customers has resulted in Plaintiff and the Missouri Subclass spending time and money to protect against identity theft. Plaintiff and the Missouri Subclass members are now at a higher risk of identity theft crimes. This harm sufficiently outweighs any justification or motives for Luxottica's practice of collecting and storing confidential and sensitive PII and PHI without the appropriate and reasonable safeguards to protect such information.

336. As a result of Luxottica's practices and conduct, Plaintiff and the Missouri Subclass members have suffered injury-in-fact and have lost money or property. As a result of Luxottica's failure to adopt, implement, and maintain reasonable security procedures, and the resulting Data Breach, Plaintiff and the Missouri Subclass members have incurred costs and spent time associated with monitoring and repairing issues from the loss of PII an PHI and issues of identity theft.

VII. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Luxottica as follows:

A. For an Order certifying the Class and Subclasses, as defined herein, and appointing Plaintiffs and Plaintiffs' counsel to represent the Class and Subclasses;

B. For injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class members, including but not limited to an order:

1) Prohibiting Luxottica from engaging in the wrongful and unlawful acts described herein;

2) Requiring Luxottica to protect, including through adequate encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

3) Requiring Luxottica to delete, destroy, and purge the PII and PHI of Plaintiffs and Class members unless Luxottica can provide the Court a reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and the Class members;

4) Requiring Luxottica to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class members' PII and PHI;

5) Requiring Luxottica to engage independent third-party security auditors and internal personnel to run automated security monitoring;

6) Requiring Luxottica to audit, test, and train its personnel regarding any new or modified procedures;

7) Requiring Luxottica to segment data by, among other things, creating firewalls and access controls so that if one area of Luxottica's network is compromised, hackers cannot gain access to other portions of Luxottica's systems;

8) Requiring Luxottica to conduct regular database scanning and security checks;

9) Requiring Luxottica to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII and PHI, as well as protecting the PII and PHI of Plaintiffs and Class members;

10) Requiring Luxottica to routinely and continually conduct internal training and education, at least annually, to inform security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

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

12) Requiring Luxottica to meaningfully educate all Class members about the threats they face as a result of the loss of their PII and PHI to third parties, as well as the steps affected individuals must take to protect themselves;

13) Requiring Luxottica to implement logging and monitoring programs sufficient to track traffic to and from its servers, as well as programs sufficient to protect infiltration of its computer and data storage systems; and

14) Requiring Luxottica to provide ten years of identity theft and fraud protection services to Plaintiffs and Class members.

C. For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;

D. For an award of statutory damages and punitive damages, as allowed by law in an amount to be determined;

E. For an award of restitution or disgorgement, in an amount to be determined;

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

G. For prejudgment interest on all amounts awarded; and

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

JURY DEMAND

Plaintiffs, on behalf of himself and the Class of all others similarly situated, hereby demands a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

DATED: January 27, 2021

ROBBINS GELLER RUDMAN & DOWD LLP

s/ Dorothy P. Antullis

Dorothy P. Antullis* (Interim Lead Counsel)
Stuart R. Davidson*
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Phone: (561) 750-3000
Fax: (561) 750-3364
dantullis@rgrdlaw.com
sdavidson@rgrdlaw.com

TYCKO & ZAVAREEI LLP
Hassan A. Zavareei* (Interim Lead Counsel)
1828 L Street NW, Suite 1000
Washington, D.C. 20036
Phone: (202) 973-0900
Fax: (202) 973-0950
hzavareei@tzlegal.com

CHESTNUT CAMBRONNE PA
Bryan L. Bleichner* (Interim Lead Counsel)
Jeffrey D. Bores*
Christopher P. Renz*
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
jbores@chestnutcambronne.com
crenz@chestnutcambronne.com

GOLDENBERG SCHNEIDER, LPA
Jeffrey S. Goldenberg (Interim Liaison Counsel)
Todd B. Naylor
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Phone: (513) 345-8297
Fax: (513) 345-8294
jgoldenberg@gs-legal.com
tnaylor@gs-legal.com

MARKOVITS, STOCK & DEMARCO, LLC
Terence R. Coates (Interim Liaison Counsel)
Zachary C Schaengold
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
zschaengold@msdlegal.com

PEARSON, SIMON & WARSHAW, LLP
Melissa S. Weiner* (Interim Executive Committee Member)
800 Lasalle Avenue, Suite 2150
Minneapolis, MN 55402
Telephone: 612/389-0600
612/389-0610 (fax)
mweiner@pswlaw.com

KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
Jonathan M. Streisfeld* (Interim Executive Committee Member)
1 West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Telephone: 954/525-4100
954/525-4300 (fax)
streisfeld@kolawyers.com

GREENWALD DAVIDSON RADBIL PLLC
Michael L. Greenwald* (Interim Executive Committee Member)
7601 N. Federal Hwy., Suite A-230
Boca Raton, FL 33487
Telephone: 561/826-5477
954/525-4300 (fax)
mgreenwald@gdrlawfirm.com

Attorneys for Plaintiffs
**Admitted Pro Hac Vice*

CERTIFICATE OF SERVICE

I hereby certify that on January 27, 2021, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF and that the foregoing document is being served on all counsel of record or parties registered to receive CM/ECF Electronic Filings.

s/ Dorothy P. Antullis
DOROTHY P. ANTULLIS