Exhibit C

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

JESSIE CROCKETT, **and** **DONNA RIVERA,** on behalf of themselves and all others similarly situated, Plaintiffs, v. **LUXOTTICA OF AMERICA INC.,** Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Jessie Crockett and Donna Rivera("Plaintiffs"), by and through their attorneys, upon personal knowledge as to themselves and their own acts and experiences, and upon information and belief as to all other matters, allege as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this Class Action Complaint ("Complaint") against Defendant Luxottica of America Inc. ("Defendant" or "Luxottica"), individually and on behalf of all others similarly situated based on Defendant's failure to properly safeguard its customers' personally identifiable information ("PII"), including current and former customer's names, phone numbers, dates of birth, Social Security numbers, email addresses, street addresses, and bank account information. Defendant also failed to properly safeguard its customers' protected health information ("PHI") exposed in the breach, including health appointment dates and time, health

insurance policy numbers, doctor or appointment notes, prescription information, health conditions, and medical procedures.

2. Luxottica owns and operates a number of service providers in the eyewear and eyecare markets. This includes well-known companies such as Pearle Vision and LensCrafters, which offer eyewear and often include optometrist offices within the same physical space. Appointments scheduled with such service providers are done through a Luxottica controlled and owned eye doctor appointment scheduling application (the "Scheduling Application.").

3. Luxottica did not adequately safeguard Plaintiffs' data within the Scheduling Application, and now they and hundreds of thousands of other patients are the victims of a significant long-lasting data breach that will affect them for years (the "Security Breach").

4. Luxottica is responsible for allowing this data breach through its failure to implement and maintain reasonable safeguards and failure to comply with industry-standard data security practices.

5. Despite its role in managing so much sensitive and personal information, during the duration of the data breach, Luxottica failed to recognize and detect unauthorized third parties accessing its computer data and storage systems, and failed to recognize the substantial amounts of data that had been compromised. This was in part because of, but also part and parcel with, Luxottica's failure to take any steps to investigate the numerous red flags, each of which individually should have told Luxottica that its systems were not secure.

6. Luxottica had numerous statutory, regulatory, contractual, and common law obligations, including those based on its affirmative representations to Plaintiffs and class members, to keep their PII, including PHI, confidential, safe, secure, and protected from unauthorized disclosure or access.

7. Plaintiffs and those similarly situated rely upon Luxottica to maintain the security and privacy of the PII and PHI entrusted to it; when providing their PII and or PHI, they reasonably expected and understood that Luxottica would comply with its obligations to keep the information secure and safe from unauthorized access.

8. In this day and age of regular and consistent data security attacks and data breaches, in particular in the healthcare industry and related services, Luxottica's Security Breach is particularly egregious.

9. As a result of Luxottica's failures, Plaintiffs and the class members are at a significant risk of identity theft, financial fraud, and/or other identity-theft or fraud, imminently and for years to come. Just as their PII and PHI was stolen because of its inherent value in the black market, now the inherent value of Plaintiffs' and the class members' PII and PHI in the legitimate market is decreased. Moreover, the injuries described were exacerbated by Luxottica's failure to timely inform and notify Plaintiffs and the class members of the data breach and their injuries. Furthermore, by failing to provide adequate notice, Luxottica prevented Plaintiffs and prospective class members from protecting themselves from the potential damages arising out of the data breach.

10. To date, Luxottica does not acknowledge the breach on its websites or provide information other than the single email or letter notifying its customers to be vigilant in monitoring their credit.

11. On information and belief, as a result of this massive data breach, as many as 829,000 or more users of Luxottica's services have suffered exposure of PII and PHI entrusted to Luxottica.

12. In addition, based on Defendant's actions, Plaintiffs and the proposed class have

received services that were and are inferior to those for which they have contracted, and have not been provided the protection and security Defendant promised when Plaintiffs and the proposed class entrusted Defendant with their PII and PHI.

13. Plaintiffs and members of the proposed class have suffered actual and imminent injuries as a direct result of the data breach. The injuries suffered by Plaintiffs and the proposed class as a direct result of the data breach include: (a) theft of their PII and PHI; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the data breach and the stress, nuisance, and annoyance of dealing with all issues resulting from the data breach; (d) the imminent injury arising from potential fraud and identity theft posed by their PII and PHI being placed in the hands of the ill-intentioned hackers and/or criminals; (e) damages to and diminution in value of their PII and PHI entrusted to Luxottica and with the mutual understanding that Luxottica would safeguard Plaintiffs' and class members' PII and PHI against theft and not allow access and misuse of their PII and PHI by others; (f) the reasonable value of the PII entrusted to Luxottica; and (g) the continued risk to their PII and PHI, which remains in the possession of Luxottica and which is subject to further breaches so long as Luxottica fails to undertake appropriate and adequate measures to protect Plaintiffs' and class members' PII and PHI in its possession.

14. Plaintiffs seek to remedy these harms, and prevent their future occurrence, on behalf of themselves and all similarly situated persons whose PII and PHI was compromised and stolen as a result of the data breach.

15. Accordingly, Plaintiffs, on behalf of themselves and other members of the class, assert claims for breach of implied contract, negligence, bailment, and unjust enrichment, and seek

injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

16. Plaintiff Crockett is a natural person and a resident of the State of Wisconsin. She and her family use Pearle Vision at 3063 Meadowlark Lane, Altoona, Wisconsin 54720 for their eye care needs, including using the Scheduling Application, to obtain appointments and eye care. 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. 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. 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.

17. Plaintiff Rivera is a natural person and resident of the State of Ohio. Plaintiff and her family have made appointments using the Scheduling Application and received eye care

treatment from the LensCrafters at 3580 Westgate, Fairview Park, Ohio 44126. She entrusted her PII, PHI, and other confidential information such as health savings account 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 had been hacked and stolen, she has suffered emotional anguish and the loss of a substantial amount of her time. 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.

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

19. Luxottica produces and licenses eyewear under a great number of well-known brands, such as Ray-Ban, Prada, Coach, and other luxury and non-luxury brands. It also operates eyewear and eyecare related service brands, such as LensCrafters, Pearle Vision, and Sunglass Hut. It also operates EyeMed Vision Care ("EyeMed"), which provides vision benefits to over 50 million Americans.

20. In conjunction with providing services to customers of LensCrafters, Pearle Vision, and other companies, Luxottica requires its customers to provide contact information (such as name, email, shipping address), and financial information, such as health services account or other credit card account information. As part and parcel of providing and/or accepting insurance, customers must also provide their dates of birth and other information, such as Social Security

numbers, that Luxottica requests.

21. Luxottica also creates electronic health records of its customers by gathering medical information of its customers. This information comes from the customers and also from other individuals or organizations, such as referring physicians, other doctors, and or insurance plans.

22. Luxottica provides that all of its affiliates are permitted to share customer PII and other information across brands.

23. Plaintiffs' injuries will be redressed by a favorable outcome in this litigation because they seek compensatory damages.

JURISDICTION & VENUE

24. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Plaintiffs (and many members of the class) and Defendant are citizens of different states.

25. This Court has general personal jurisdiction over Luxottica because Luxottica's principal place of business is in Mason, Ohio.

26. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(a)(2), 1391(b)(1) and (2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, Luxottica resides in this District and is the sole Defendant, and Luxottica conducts substantial business in this District.

FACTUAL ALLEGATIONS

27. Luxottica is the market leader in eyewear and eyecare in the United States. At the end of the fourth quarter of calendar 2019, it claimed to have almost 4,000 physical stores in North

America, including over 1,000 LensCrafters and over 100 Pearle Vision stores.[1]

28. EyeMed provides vision benefits to over 50 million Americans. As with all benefit or insurance companies, upon information and belief, this requires disclosure of PII and PHI to Luxottica by all these members.

29. Luxottica is fully aware of how sensitive the PII and PHI it stores and maintains is. It is also aware of how much PII and PHI it collects, uses, and maintains from each Plaintiff or class member. Luxottica offers services related to healthcare treatment and the provision of insurance.

30. By requiring the production of, collecting, obtaining, using, and deriving benefits from Plaintiffs' and the class members' PII and PHI, Luxottica assumed certain legal and equitable duties and knew or should have known that it was responsible for the diligent protection of the PII and PHI it collected and stored.

Luxottica knew that it was and continues to be a prime target for cyberattacks

31. Luxottica knew that it was an ideal target for hackers and those with nefarious purposes related to consumers' data. It processed and saved multiple types and many levels of PII and PHI through its many types of businesses.

32. 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.

33. Through companies like LensCrafters and Pearle Vision, Luxottica processed

[1] https://www.statista.com/statistics/241663/number-of-stores-of-luxottica-in-northamerica/#:~:text=As%20of%20December%2031%2C%202019,corporate%20stores%20in%20North%20America (last visited December 14, 2020).

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, health savings account information, credit card and other payment information, email and home addresses, and other PII.

34. 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 the consumers' preferences.

35. The seriousness with which Luxottica should have taken its data security is shown by the number of data breaches perpetrated in the healthcare and retail industries in the last few years.

36. Despite knowledge of the prevalence of healthcare and retail data breaches, Luxottica failed to prioritize its customers' data security by implementing reasonable data security measures to detect and prevent unauthorized access to the millions upon millions of sensitive data points of its customers. As a highly successful vertically integrated eyewear and eyecare company, Luxottica had the resources to invest in the necessary data security and protection measures.

37. It did not. Luxottica failed to undertake adequate analyses and testing of its own systems, adequate personnel training, and other data security measures to avoid the failures presented to customers in late October 2020 but which occurred several months earlier.

38. Despite its awareness, Luxottica did not take the necessary and required minimal steps to secure Plaintiffs' and the class members' PII and PHI. As a result, hackers breached and stole important PII and PHI from almost one million Luxottica customers in early August 2020.

39. Between three and four months later (late October to late November 2020), Luxottica informed Plaintiffs and members of the class by mail and email it had "learned of an

issue impacting our online eye doctor appointment scheduling application." For example, Plaintiff Rivera received the following in an email on or about November 30, 2020:

> You are receiving this notice because an appointment was made or treatment was received from an eye care clinic run by […]. Based on our investigation, we have determined that the personal information involved in this incident may have included your: 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. Luxottica is not aware of any misuse of personal information or harm to patients as a result of this incident. [Emphasis added]

40. Luxottica's disclosure letter described what it was doing to remedy the situation:

> We began working with third-party cybersecurity specialists to determine the full nature and scope of the event and develop a remediation plan to prevent this type of incident from happening again. We have taken measures designed to enhance our security controls and prevent this type of incident from recurring, including implementing additional access restrictions on our patient scheduling platform. We also notified federal law enforcement of this matter.

41. Notably, the "measures" Luxottica refers to are only promised to be "designed" to increase security and prevent another breach, not to actually prevent another breach.

42. Luxottica "regret[s] any inconvenience or concern this incident may cause" Plaintiffs and the class members, and encourages them to "always remain vigilant," and if they see "suspicious or unusual activity," not to tell Luxottica, but to report it to someone else.

43. If Plaintiffs or class members go to the website set up by data incident response vendor Kroll on behalf of Luxottica, they are told the same thing: be vigilant, Luxottica hasn't seen anything bad happen yet, and for a small set of victims that Luxottica knows had their Social Security number or certain medical information stolen, Luxottica will offer "complimentary access to identity monitoring services."

44. Despite knowing since early August that there had been a data breach, confirmed by the end of August, Luxottica did not issue notice to those affected within the timeframe required

by statute.

45. It did disclose to the United States Department of Health and Human services that the data breach included at least 829,454 patients.

46. Despite Luxottica's attempts to suggest that there is little to be afraid of, a month after Luxottica discovered the August 2020 data breach, hackers succeeded in another attack on Luxottica's parent company. This attack, in September 2020 and well after Luxottica should have immediately remedied its cybersecurity failures, involved many of Luxottica's main websites, such as LensCrafters, EyeMed, Pearle Vision, and Sunglass Hut, which were taken down by hackers, followed soon by a deposit on the dark web of an enormous collection of confidential information from Luxottica's parent company's personnel and finance departments.

47. These two breaches, within two months, suggest Luxottica's pervasive inability to adequately protect PII and PHI.

Luxottica owed a duty to Plaintiffs and class members to adequately safeguard their PII and to provide timely notice of the breach of its systems

48. Luxottica knows the importance of security in maintaining personal information, and the value its users place on keeping their PII and PHI secure.

49. Luxottica owes a duty to Plaintiffs and the class members to maintain adequate security and to protect the confidentiality of their PII and PHI.

50. Luxottica owes a further duty to its current and former users to immediately and accurately notify them of a breach of its systems to protect them from identity theft and other misuse of their PII and PHI.

The sort of PII at issue here is particularly valuable to hackers

51. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However,

information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of frauds.

52. The unauthorized disclosure of Social Security numbers can be particularly damaging, because Social Security numbers cannot easily be replaced. In order to obtain a new number a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, no new number can be obtained until the damage has been done.

53. Furthermore, as the Social Security Administration ("SSA") warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[2]

54. Here, the unauthorized access by the hackers left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. The PII and PHI of Plaintiffs and class members stolen in the Luxottica Security Breach constitutes a dream for hackers and a nightmare for Plaintiffs and the class. Plaintiffs' and class members' stolen PII and PHI represents essentially one-stop shopping for

[2] SSA, Identity Theft and Your Social Security Number, SSA Publication No. 05-10064 (Dec. 2013), *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Nov. 13, 2020).

identity thieves.

55. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[3] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[4]

56. More recently the FTC has released its updated publication on protecting PII for businesses, which include instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

57. The FTC has, upon information and belief, brought enforcement actions against businesses for failing to protect customers' PII. The FTC has done this by taking a failure to employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. § 45.

58. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to the GAO Report

> [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

[3] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited Nov. 13, 2020).

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

from data breaches cannot necessarily rule out all future harm.[5]

59. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post for sale stolen credit card numbers, Social Security numbers, and other PII on a number of Internet websites. Plaintiffs' and class members' PII and PHI that was stolen has a high value on both legitimate and black markets.

60. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[6]

61. Consumers place a high value not only on their PII, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable.

62. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[7] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive

---

[5] *See* http://www.gao.gov/new.items/d07737.pdf at 29 (last visited Nov. 13, 2020).
[6] FEDERAL TRADE COMMISSION, *The Information Marketplace: Merging and Exchanging Consumer Data*, *transcript available* at http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data (last visited Nov. 13, 2020).
[7] Hann, Hui, *et al*, The Value of Online Information Privacy: Evidence from the USA and Singapore, at 17. Oct. 2002, *available at* https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Nov. 13, 2020).

the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII to bad actors—would be much higher today.

63. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent refund. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

64. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Former and current users of Luxottica systems whose Social Security numbers have been compromised will and already have spent time contacting various agencies, such as the Internal Revenue Service and the Social Security Administration. They also now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number, and will need to monitor their credit and tax filings for an indefinite duration.

65. Again, because the information Luxottica allowed to be compromised and taken is of such a durable and near-permanent quality, the harms to Plaintiffs and the class will continue to grow, and Plaintiffs and the class will continue to be at substantial risk for further imminent and future harm.

Luxottica's post-breach activity was inadequate

66. Personal, health, and financial information can be sold on the black-market almost immediately. As Illinois Attorney General Lisa Madigan aptly put it, "the second somebody gets your credit or debit card information, it can be a matter of hours or days until it's sold on the black

market and someone's starting to make unauthorized transactions."[8] Thus, the compromised information could be used weeks prior to the receipt of any letter from Luxottica and Luxottica's proposed solutions to the potential fraud are, therefore, woefully deficient.

67. Immediate notice of a security breach is essential to protect people such as Plaintiff and the class members. Luxottica failed to provide such immediate notice, in fact taking at least three to four months to disclose that there had been a breach, thus further exacerbating the damages sustained by Plaintiffs and the class resulting from the breach.

68. Such failure to protect Plaintiffs' and the class members' PII and PHI, and timely notify of the breach, has significant ramifications. The information stolen allows criminals to commit theft, identity theft, and other types of fraud. Moreover, because of many of the data points stolen are persistent—for example, Social Security number, name, address, email address, and medical history—as opposed to transitory—for example, the date of an appointment, criminals who purchase the PII and PHI belonging to Plaintiffs and the class members do not need to use the information to commit fraud immediately. The PII and PHI—already organized in Luxottica's databases—can be used or sold for use years later.

69. A single person's PHI can fetch up to $350 on the dark web, in part valuable because of the scope and comprehensiveness of the data and information, which can be used to steal identities for illegal drug or medical purchases or defraud insurers. Allowing hackers to steal this type of information is particularly nefarious, as many banks or credit card providers have substantial fraud detection systems with quick freeze or cancellation programs in place, whereas the breadth and usability of PHI allows criminals to get away with misuse for years before

[8] Phil Rosenthal, *Just assume your credit and debit card data were hacked*, http://www.chicagotribune.com/business/columnists/ct-data-breach-credit-scam-rosenthal-1001-biz-20140930-column.html#page=1 (last visited Nov. 13, 2020).

healthcare-related fraud is spotted.

70. Every year, victims of identity theft lose billions of dollars. Reimbursement is only the beginning, as these victims, at a minimum, usually spend hours and hours attempting to repair the impact to their credit.

71. This is in addition to the ongoing attention victims such as Plaintiffs and the class members spend attempting to monitor and/or repair hacked data. Plaintiffs have each spent hours reading communications from Luxottica, reading information published about Luxottica that explains that Luxottica's three or four month later response was not sufficient and that Luxottica is downplaying the number of Social Security numbers stolen, 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 will continue to spend time and resources reviewing bank statements, health savings account statements, and ongoing notices from insurers and healthcare providers to try to protect themselves against medical fraud.

72. Plaintiffs and the class members are at constant risk of imminent and future fraud, misuse of their PII and PHI, and identity theft for many years in the future as a result of Luxottica's actions and the data breach. They have suffered real and tangible loss, including but not limited to the loss in the inherent value of their PII and PHI, the loss of their time as they have had to spend additional time monitoring accounts and activity, and additional economic loss to mitigate the costs of injuries realized as a result of discovery in this case, but hitherto kept deliberately hidden by Luxottica.

CLASS ACTION ALLEGATIONS

73. Plaintiffs bring all claims as class claims under Federal Rule of Civil Procedure

23. The requirements of Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3) are met with respect to the class defined below.

74. Under Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action as a national class action for themselves and all members of the following class of similarly situated persons:

The Nationwide Class

> All persons who reside in the United States whose PII and PHI was compromised as a result of the security breach first disclosed by Luxottica on October 27, 2020.

75. Excluded from the class are Defendant; officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

76. Plaintiffs reserve the right to modify and/or amend the Class definition, including but not limited to creating subclasses, as necessary.

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

78. All members of the proposed class are readily ascertainable in that Luxottica has access to addresses and other contact information for all members of the class, which can be used for providing notice to class members.

79. ***Numerosity***. The class is so numerous that joinder of all members is impracticable. The class includes as many as 829,000 individuals whose PII and PHI was compromised by the Luxottica Security Breach.

80. ***Commonality***. There are numerous questions of law and fact common to Plaintiffs and the class, including the following:

- whether Luxottica engaged in the wrongful conduct alleged in this Complaint;
- whether Luxottica's conduct was unlawful;
- whether Luxottica failed to implement and maintain reasonable systems and security procedures and practices to protect customers' PII and PHI;
- whether Luxottica unreasonably delayed in notifying affected customers of the Security Breach;
- whether Luxottica owed a duty to Plaintiffs and members of the class to adequately protect their PII and PHI and to provide timely and accurate notice of the Luxottica Security Breach to Plaintiffs and members of the class;
- whether Luxottica breached its duties to protect the PII and PHI of Plaintiffs and members of the class by failing to provide adequate data security and failing to provide timely and adequate notice of the Luxottica Security Breach to Plaintiffs and the class;
- whether Luxottica's conduct was negligent;
- whether Luxottica knew or should have known that its computer systems were vulnerable to attack;
- whether Luxottica's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of class members' PII and PHI;
- whether Luxottica wrongfully or unlawfully failed to inform Plaintiffs and members of the class that it did not maintain computers and security practices adequate to reasonably safeguard customers' financial and PII and PHI;
- whether Luxottica should have notified the public, Plaintiffs, and class members immediately after it learned of the Security Breach;
- whether Plaintiffs and members of the class suffered injury, including ascertainable losses, as a result of Luxottica's conduct (or failure to act);
- whether Luxottica breached its duties to Plaintiffs and the class as a bailee of PII and PHI entrusted to it and for which Luxottica owed a duty to safeguard and of safekeeping;
- whether Plaintiffs and members of the class are entitled to recover damages;

- whether Plaintiffs and class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

81. ***Typicality***. Plaintiffs' claims are typical of the claims of the class in that Plaintiffs, like all class members, had their PII and PHI compromised, breached, and stolen in the Luxottica Security Breach. Plaintiffs and all class members were injured through the uniform misconduct of Luxottica described in this Complaint and assert the same claims for relief.

82. ***Adequacy***. Plaintiffs and counsel will fairly and adequately protect the interests of the class. Plaintiffs have retained counsel who are experienced in class action and complex litigation. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of other members of the class.

83. ***Predominance***. The questions of law and fact common to class members predominate over any questions which may affect only individual members.

84. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most class members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Luxottica's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the class. Plaintiffs and class members have been harmed by Luxottica's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Luxottica's conduct and/or inaction. Plaintiffs know of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

85. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual

members of the class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

86. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Luxottica. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each class member.

COUNT I — NEGLIGENCE

87. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth here.

88. Luxottica owed a duty to Plaintiffs and members of the class to safeguard the sensitive PII and PHI that they were required to provide Luxottica as a condition of receiving Luxottica's services. Luxottica was required to prevent foreseeable harm to Plaintiffs and the class members, and therefore had a duty to take reasonable steps to safeguard sensitive PII and PHI from unauthorized release or theft.

89. In other words, Luxottica was required to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their personal, health, and financial information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Luxottica's security systems to ensure that Plaintiffs' and class members' personal, health, and financial information in Luxottica's possession was adequately secured and protected.

90. Luxottica further owed a duty to Plaintiffs and class members to implement

processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts.

91. There is a very close connection between Luxottica's failure to follow reasonable security standards to protect its current and former users' PII and PHI and the injury to Plaintiffs and the class. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

92. If Luxottica had taken reasonable security measures, data thieves would not have been able to take the personal information of as many as 829,000 current and former users of Luxottica's services. The policy of preventing future harm weighs in favor of finding a special relationship between Luxottica and Plaintiffs and the class. If companies are not held accountable for failing to take reasonable security measures to protect their customers' PII and PHI, they will not take the steps that are necessary to protect against future security breaches.

93. Luxottica owed a duty to timely disclose the material fact that Luxottica's computer systems and data security practices were inadequate to safeguard users' personal, health, and financial data from theft.

94. Luxottica breached these duties by the conduct alleged in the Complaint by, including without limitation, failing to protect its customers' personal, health, and financial, information; failing to maintain adequate computer systems and data security practices to safeguard customers' personal, health, and financial information; failing to disclose the material fact that Luxottica's computer systems and data security practices were inadequate to safeguard customers' personal, health, and financial data from theft; and failing to disclose in a timely and

accurate manner to Plaintiffs and members of the class the material fact of the data breach.

95. As a direct and proximate result of Luxottica's failure to exercise reasonable care and use commercially reasonable security measures, the PII and PHI of current and former Luxottica users was accessed by ill-intentioned criminals who could and will use the information to commit identity fraud or debit and credit card fraud. Plaintiffs and the class face the imminent, certainly impending and substantially heightened risk of identity theft, fraud and further misuse of their PII and PHI.

96. As a proximate result of this conduct, Plaintiffs and the other class members suffered damage after the unauthorized data release and will continue to suffer damages in an amount to be proven at trial. Furthermore, Plaintiffs and the class have suffered emotional distress as a result of the breach and have lost time and/or money as a result of past and continued efforts to protect their PII and PHI and prevent the unauthorized use of their PII and PHI.

COUNT II — BAILMENT

97. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth here.

98. Plaintiffs and the class delivered their personal, health, and financial information to Luxottica for the exclusive purpose of obtaining services.

99. The PII and PHI is intangible personal property belonging to Plaintiffs and the class members.

100. In delivering their PII and PHI to Luxottica, Plaintiffs and class members intended and understood that Luxottica would adequately safeguard their PII and PHI.

101. Luxottica accepted possession of Plaintiffs' and class members' PII and PHI.

102. By accepting possession of Plaintiffs' and class members' PII and PHI, Luxottica

understood that Plaintiffs and class members expected Luxottica to adequately safeguard their PII and PHI. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

103. During the bailment (or deposit), Luxottica owed a duty to Plaintiffs and class members to exercise reasonable care, diligence, and prudence in protecting their PII and PHI as well as a duty to safeguard personal information properly and maintain reasonable security procedures and practices to protect such information. Defendant breached this duty.

104. Luxottica breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and class members' personal, health, and financial information, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and class members' personal, health, and financial information.

105. As a proximate result of this conduct, Plaintiffs and the other class members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT III — BREACH OF IMPLIED CONTRACT

106. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth here.

107. Plaintiffs and the class delivered their personal, health, and financial information to Luxottica as part of the process of obtaining services provided by Luxottica.

108. Plaintiffs and members of the class entered into implied contracts with Luxottica pursuant to which Luxottica agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and class members that their data had been breached and compromised.

109. In providing such data, Plaintiffs and the other members of the class entered into an implied contract with Luxottica whereby Luxottica became obligated to reasonably safeguard Plaintiffs' and the other class members' sensitive, non-public information.

110. In delivering their PII and PHI to Luxottica, Plaintiffs and class members intended and understood that Luxottica would adequately safeguard their PII and PHI.

111. Plaintiffs and the class members would not have entrusted their private and confidential financial, health, and personal information to Defendants in the absence of such an implied contract.

112. Luxottica accepted possession of Plaintiffs' and class members' PII and PHI for the purpose of providing services to Plaintiffs and class members.

113. Had Luxottica disclosed to Plaintiffs and members of the class that Luxottica did not have adequate computer systems and security practices to secure users' and former users' PII and PHI, Plaintiffs and members of the class would not have provided their PII and PHI to Luxottica.

114. Luxottica recognized that its users' and former users' PII and PHI is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and members of the class.

115. Plaintiffs and members of the class fully performed their obligations under the implied contracts with Luxottica.

116. Luxottica breached the implied contract with Plaintiffs and the other members of the class by failing to take reasonable measures to safeguard their data.

117. As a proximate result of this conduct, Plaintiffs and the other class members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV — UNJUST ENRICHMENT

118. Plaintiffs incorporates by reference those paragraphs set out above as if fully set forth herein.

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

120. The monies or fees paid by the 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.

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

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

123. 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' personal, health, and financial information that they paid for but did not receive.

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

125. Luxottica's enrichment at the expense of Plaintiffs and class members is and was unjust.

126. As a result of Luxottica's wrongful conduct, as alleged above, Plaintiffs and the class 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.

RELIEF REQUESTED

Plaintiffs, individually and on behalf of the proposed class, request that the Court:

1. Certify this case as a class action on behalf of the class defined above, appoint Plaintiffs as class representatives, and appoint the undersigned counsel as class counsel;

2. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and other class members;

3. Award restitution and damages to Plaintiffs and class members in an amount to be determined at trial;

4. Award Plaintiffs and class members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;

5. Award Plaintiffs and class members pre- and post-judgment interest, to the extent allowable; and

6. Award such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of any and all issues in this action so triable of right.

Respectfully submitted,

/s/ Terence R. Coates
W.B. Markovits (0018514)
Terence R. Coates (0085579)
Zachary C Schaengold (0090953)
Dylan J. Gould (0097954)
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
bmarkovits@msdlegal.com
tcoates@msdlegal.com
zschaengold@msdlegal.com
dgould@msdlegal.com

Bryan L. Bleichner (pro hac vice forthcoming)
Jeffrey D. Bores (pro hac vice forthcoming)

Christopher P. Renz (pro hac vice forthcoming)
CHESTNUT CAMBRONNE, PA
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

Counsel for Plaintiffs and the Class