

David S. Casey, Jr., SBN 060768
dcasey@cglaw.com

Gayle M. Blatt, SBN 122048
gmb@cglaw.com

Jeremy Robinson, SBN 188325
jrobinson@cglaw.com

P. Camille Guerra, SBN 326546
camille@cglaw.com

Catherine McBain, SBN 303911
kmcbain@cglaw.com

CASEY GERRY SCHENK
FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Tel: (619) 238-1811; Fax: (619) 544-9232

Attorneys for Plaintiff ANJANETTE RAMEY and the Class

Patrick N. Keegan, Esq., SBN 167698
pkeegan@keeganbaker.com

KEEGAN & BAKER, LLP
2292 Faraday Avenue, Suite 100
Carlsbad, CA 92008
Telephone: (760) 929-9303
Facsimile: (760) 929-9260

Attorneys for Plaintiff JANE DOE and the Class and SubClass

SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF SAN DIEGO, CENTRAL DIVISION

ANJANETTE RAMEY, and JANE DOE,
on behalf of themselves and all other
persons similarly situated,

Plaintiffs,

v.

TOTAL VISION, LLC., a Delaware
limited liability company; JOHN C.
PACK, O.D. AND BEVERLY BIANES,
O.D., INC.; JOHN C. PACK, O.D.;
BEVERLY BIANES, O.D.; and DOES 1
through 100,

Defendants.

ELECTRONICALLY FILED
Superior Court of California,
County of San Diego

11/18/2021 at 01:08:00 PM

Clerk of the Superior Court
By Taylor Crandall, Deputy Clerk

CASE NO. 37-2021-00002017-CU-MC-CTL

[consolidated with Case No.
37-2021-00018344-CU-BT-CTL]

Hon. Carolyn Caietti

**AMENDED CONSOLIDATED CLASS
ACTION COMPLAINT**

Demand for Jury Trial

1 Plaintiff Anjanette Ramey and Plaintiff Jane Doe¹ (collectively referred to as
2 “Plaintiffs” unless otherwise specified), by and through their attorneys, on behalf of
3 themselves and all others similarly situated, hereby bring this class action and
4 Amended Consolidated Class Action Complaint against Defendant Total Vision,
5 LLC; and Jane Doe brings this action on behalf of SubClass members who were
6 patients of John C. Pack, O.D. and Beverly Bienes, O.D., Inc.; John C. Pack, O.D.,
7 Beverly Bienes, O.D., and DOES 1-100 (collectively referred to as “Defendants”
8 unless otherwise specified), and allege as follows:

9 INTRODUCTION

10 1. Defendant Total Vision, LLC is a limited liability company that owns
11 and operates a network of optometry centers throughout California. It describes
12 itself on its website as “the leading network of optometry providers in California.”

13 2. Plaintiff Anjanette Ramey is and at all times relevant was, a patient at
14 TVC Tierrasanta, one of Total Vision’s optometry centers. She, and the other Class
15 (defined *infra*) members, are “patients” of Defendant Total Vision, LLC as defined
16 in Civil Code § 56.05, subd. (k).

17 3. Plaintiff Jane Doe is and at all times relevant was, a patient of John C.
18 Pack, O.D. and Beverly Bienes, O.D., Inc., John C. Pack, O.D., Beverly Bienes, O.D.
19 She, and the other SubClass (defined *infra*) members, are “patients” of Defendants
20

21 ¹ California statutory law specifically allows a party to bring a lawsuit using a pseudonym
22 in cases involving health care patients. Cal. Civ. Code § 3427.3 (West 2011). Specifically,
23 section 3427.3 provides, “The court having jurisdiction over a civil proceeding under this
24 title shall take all steps *reasonably necessary to safeguard the individual privacy and*
25 *prevent harassment of a health care patient*, licensed health practitioner, or employee,
26 client, or customer of a health care facility who is a party or witness in the proceeding,
27 including granting protective orders. *Health care patients*, licensed health practitioners,
28 and employees, clients, and customers of the health care facility *may use pseudonyms to*
protect their privacy.” Cal. Civ. Code § 3427.3 (emphasis added). Here, a pseudonym has
been used in place of the real name of Plaintiff because at all times relevant to this action,
Plaintiff is a health care patient under Civil Code § 56.05(k) and has individual privacy
concerns and a reasonable fear of harassment in light of the nature of the case.

1 John C. Pack, O.D. and Beverly Bienes, O.D., Inc., John C. Pack, O.D., Beverly
2 Bienes, O.D. as defined in Civil Code § 56.05, subd. (k).

3 4. This class action arises from Defendants' negligence and failure to
4 properly create, maintain, preserve, and/or store confidential, medical and
5 personal identifying information of Plaintiffs and all other persons similarly
6 situated. As a direct result of Defendants' negligence and failures, an unauthorized
7 person or persons gained access to a computer database server of one or more of
8 the Defendants on or about October 30, 2020, causing at least one unauthorized
9 person access to, view, exfiltrate, steal and/or disclose unencrypted medical and
10 personal identifying information – including names, addresses, dates of birth,
11 social security numbers, and prescription information – of Plaintiffs and others
12 similarly situated – in violation of the Confidentiality of Medical Information Act,
13 Civil Code §§ 56, *et seq.* (hereinafter referred to as the "CMIA"), the Security
14 Notification Laws, Civil Code § 1798.82, and the Business and Professions Code
15 §§ 17200 *et seq.* Under the CMIA, Plaintiffs, and all others similarly situated, have
16 the right to expect the confidentiality of their medical information in Defendants'
17 possession, and/or derived from Defendants, to be reasonably preserved and
18 protected from unauthorized access, viewing, exfiltration, theft, and/or disclosure.

19 5. As alleged more fully below, by failing to take adequate and reasonable
20 measures to ensure its data systems were protected against unauthorized
21 intrusions, failing to invest in cyber security and data protection safeguards,
22 failing to implement adequate and reasonable security controls and user
23 authorization and authentication processes, failing to limit the types of data
24 permitted to be transferred, failing to properly and adequately educate and train
25 its employees, and failing to put into place reasonable or adequate computer
26 systems and security practices to safeguard customers' and patients' medical and
27 personal identifying information, Defendants negligently created, maintained,
28 preserved, and stored Plaintiffs' and the Class (defined *infra*) members' medical

1 and personal identifying information in possession of or derived from Defendants
2 allowed such information to be accessed and viewed by at least one unauthorized
3 third party, without Plaintiffs' and the Class members' prior written authorization,
4 which constitutes unauthorized disclosure and/or release of their information in
5 violation of Civil Code §§ 56.10(a) and 56.101(a) of the CMIA.

6 6. In fact, Defendant Total Vision, LLC's form letter, entitled "*Important*
7 *Security Notification*," dated December 4, 2020, sent to Plaintiffs and all others
8 similarly situated, stated in part:

9 "We are contacting you regarding a data security incident
10 that has occurred on October 30, 2020 at Total Vision, LLC.
11 This incident involved your name, address, date of birth,
12 social security number, and contact lens or eyeglass
13 prescription. As a result, your personal information may
14 have been potentially exposed to others [¶] This
15 information was located on a server that was accessed by a
16 third party. Upon learning of this incident, we promptly
secured the server and then encrypted the information on
the server. Our investigation is ongoing at this time."

17 An exemplar of Defendant Total Vision, LLC's "*Important Security Notification*"
18 form letter submitted to the Attorney General of the State of California is attached
19 hereto as **Exhibit A**. The incident described in Defendant Total Vision, LLC's
20 "*Important Security Notification*" form letter is referred to herein as the
21 "Data Breach."

22 7. As a direct result of Defendant Total Vision, LLC's failure to provide
23 adequate data security, Plaintiffs' and the Class' PII has been exposed to those
24 who should not have access to it. Plaintiffs and the Class have suffered cognizable
25 damages and are now at much higher risk of identity theft and for cybercrimes of
26 all kinds.

27 8. Indeed, as a result of the Data Breach, Plaintiff Anjanette Ramey has
28 experienced numerous instances of identity fraud or attempted identity fraud,

1 including someone fraudulently purchasing an Apple iMac using her Amazon
2 account, multiple efforts to hack her email address from locations in foreign
3 countries, including one where the hacker created a folder called "Wells Fargo,"
4 and another spoof email sent to all her contacts asking for Apple gift cards, being
5 declined for a credit card despite having excellent credit history, receiving
6 fraudulent voicemails about purchases and money transfers she did not make, and
7 having difficulties with her business payment system that is connected to her
8 email address. Also, since being notified of the Data Breach, Plaintiff Ramey has
9 spent numerous hours addressing credit report and financial account issues,
10 signed up for text alerts for her credit cards and has spent additional time she
11 otherwise would have been able to use doing other things. Plaintiff Ramey has
12 spent both time and money dealing with these instances of fraud or attempted
13 fraud and will continue to have to do so in the future. Additionally, based on these
14 events and the fact that her PII is clearly in the hands of the wrong parties, she
15 remains at a very much increased risk of identity theft.

16 9. As a result of Data Breach, Plaintiff Jane Doe reasonably fears that
17 disclosure and/or release of her medical information created, maintained,
18 preserved and/or stored on Defendants' computer networks could subject her to
19 harassment, abuse, identity theft, and/or fraud. Also, since being notified of the
20 Data Breach, Plaintiff Doe has spent time addressing the Data Breach – time she
21 otherwise would have been able to use doing other things. Additionally, based on
22 these events and the fact that her PII is clearly in the hands of the wrong parties,
23 she remains at a very much increased risk of identity theft.

24 10. Because Plaintiffs' and the Class members' individually identifiable
25 medical information and other personal identifying information (collectively
26 referred to as "PII") was subject to unauthorized access and viewing by at least
27 one unauthorized third party and in violation of the CMIA, Plaintiffs, on behalf of
28 themselves and all others similarly situated, seek from Defendants nominal

1 damages in the amount of one thousand dollars (\$1,000) for each violation under
2 Civil Code §56.36(b)(1) and actual damages, according to proof, for each violation
3 pursuant to Civil Code § 56.36(b)(2). Further, because Plaintiffs also allege
4 Defendants' conduct violates Business & Professions Code §§ 17200, *et seq.*,
5 Plaintiffs, on behalf of themselves and all others similarly situated, seeks
6 injunctive relief and restitution from Defendants under Business and Professions
7 Code § 17203.

8 11. This action, if successful, will enforce an important right affecting the
9 public interest and would confer a significant benefit, whether pecuniary or
10 non-pecuniary, on a large class of persons. Private enforcement is necessary and
11 places a disproportionate financial burden on Plaintiffs in relation to Plaintiffs'
12 stake in the matter, and therefore class certification is appropriate in this matter.

13 **THE PARTIES**

14 **A. Defendants**

15 12. Defendant Total Vision, LLC ("TOTAL VISION") is a Delaware limited
16 liability company, is registered to do business and does business in the State of
17 California (Sec. of State File No. 201811010564), with its principal place of business
18 at 27271 Las Ramblas, Mission Viejo, California, 92691. TOTAL VISION is a
19 provider of optometry services and describes itself as "the leading network of
20 optometry providers in California."

21 13. TOTAL VISION is owned by Bregal Partners, a global private equity
22 firm. On its website, TOTAL VISION represents that it has "Over 75 doctors with
23 35 locations" in California and that "Total Vision providers offer primary eye care
24 services including prescription glasses, contact lenses, evaluation of ocular health,
25 emergency visits, and LASIK consultations."² On its website, TOTAL VISION
26 states that "Total Vision optometry offices provide world-class vision care. Our
27

28 ² (<https://yourtotalvision.com>, last visited April 21, 2021).

1 network of providers meet our standards for professionalism and quality, and
2 offer advanced testing and treatment.”³

3 14. At all times relevant to this action, TOTAL VISION was and is a
4 “licensed health care provider” or “provider of health care” as defined in Civil
5 Code § 56.05, subds. (h) and (m), a “contractor” under Civil Code § 56.05,
6 subd. (d), and/or “engaged in the business of furnishing administrative services to
7 programs that provide payment for health care services” under Civil Code § 56.26,
8 subd. (a), and maintained and continues to maintain “medical information” within
9 the meaning of Civil Code § 56.05, subd. (j), of Plaintiffs, the Class (defined *infra*)
10 and the SubClass (defined *infra*), including their names, addresses, dates of birth,
11 social security numbers, and contact lens or eyeglass prescriptions, and is subject
12 to the requirements and mandates of the CMIA, including but not limited to Civil
13 Code §§ 56.10, 56.101 and 56.36.

14 15. At all times relevant to this action, TOTAL VISION was and is a
15 “business” within the meaning of Civil Code § 1798.140(c)(1), owns or licenses
16 computerized data which includes Plaintiffs’ and the Class’ (defined *infra*)
17 personal information, within the meaning of Civil Code § 1798.82(h), collected
18 Plaintiff’s and the Class’ personal information within the meaning of Civil Code
19 § 1798.81.5(d)(1)(A).

20 16. Defendant John C. Pack, O.D. and Beverly Bianes, O.D., Inc. (“PACK
21 AND BIANES”), doing business as Pack and Bianes Vision Care⁴ and Pack and
22 Bianes Vision Care Optometry,⁵ is a California corporation, organized or operated
23 for the profit or financial benefit of its shareholders. PACK AND BIANES is
24 registered to do business and does business in the State of California (CA Corp.
25 No. C2299824), with its principal business office located at 890 Eastlake Parkway,
26

27 ³ (<https://yourtotalvision.com/about/>, last visited April 22, 2021).

28 ⁴ (<https://www.packandbianesvision.com/>, last visited April 22, 2021).

⁵ (<https://yourtotalvision.com/eastlake/>, last visited April 22, 2021).

1 #102, Chula Vista, CA 91914. Its registered agent of service of process located at
2 401 West A Street, #2350, San Diego, CA 92101.

3 17. At all times relevant to this action, PACK AND BIANES was and is a
4 “licensed health care provider” or “provider of health care” as defined in Civil
5 Code § 56.05, subds. (h) and (m), a “contractor” under Civil Code § 56.05,
6 subd. (d), and/or an authorized recipient of medical information, as that term is
7 defined and set forth in the CMIA, including the names, addresses, dates of birth,
8 social security numbers, and contact lens or eyeglass prescriptions of Plaintiff and
9 the SubClass (defined *infra*), and is subject to the requirements and mandates of
10 the CMIA, including but not limited to Civil Code §§ 56.10, 56.101 and 56.36. At
11 all times relevant to this action, PACK AND BIANES was and is a TOTAL VISION
12 “provider” of health care and employed and employs persons located in the
13 County of San Diego and in this judicial district.

14 18. At all times relevant to this action, PACK AND BIANES was and is a
15 “business” within the meaning of Civil Code § 1798.140(c)(1), owns or licenses
16 computerized data which includes Plaintiff Jane Doe’s and the SubClass’ personal
17 information, within the meaning of Civil Code § 1798.82(h), collected Plaintiff’s
18 and the SubClass’ personal information within the meaning of Civil Code
19 § 1798.81.5(d)(1)(A).

20 19. Defendant John C. Pack, O.D. and Defendant Beverly Bianes, O.D.,
21 together doing business as Pack and Bianes Vision Care⁶ and Pack and Bianes
22 Vision Care Optometry,⁷ with their principal business office located at 890 Eastlake
23 Parkway, #102, Chula Vista, CA 91914.

24 20. At all times relevant to this action, Defendant Pack and Defendant
25 Bianes were and are each a “licensed health care provider” or “provider of health
26 care” as defined in Civil Code § 56.05, subds. (h) and (m), a “contractor” under
27

28 ⁶ (<https://www.packandbianesvision.com/>, last visited April 22, 2021).

⁷ (<https://yourtotalvision.com/eastlake/>, last visited April 22, 2021).

1 Civil Code § 56.05, subd. (d), and/or authorized recipient of medical information,
2 as that term is defined and set forth in the CMIA, including the names, addresses,
3 dates of birth, social security numbers, and contact lens or eyeglass prescriptions
4 of Plaintiff and the SubClass (defined *infra*), and are subject to the requirements
5 and mandates of the CMIA, including but not limited to Civil Code §§ 56.10,
6 56.101 and 56.36.

7 **B. Plaintiffs**

8 21. Plaintiff Anjanette Ramey (or “Ramey”) is a resident of San Diego,
9 California. In early December 2020, Plaintiff Ramey received a notice from TOTAL
10 VISION, dated December 4, 2020, stating it improperly exposed her PII to
11 unauthorized third parties. Specifically, Plaintiff Anjanette Ramey received a letter
12 addressed to her, sent on TOTAL VISION’s behalf, entitled “*Important Security*
13 *Notification*,” dated December 4, 2020, signed by Doug Cannon, Chief Financial
14 Officer, for TOTAL VISION, stating, in part:

15 We are contacting you regarding a data security incident
16 that has occurred on October 30, 2020 at Total Vision, LLC.
17 This incident involved your name, address, date of birth,
18 social security number, and contact lens or eyeglass
19 prescription. . . . [¶] This information was located on a server
20 that was accessed by a third party. Upon learning of this
21 incident, we promptly secured the server and then
22 encrypted the information on the server. Our investigation
23 is ongoing at this time.

24 22. Prior to October 30, 2020, Ramey provided her PII to TOTAL VISION as
25 a part of a transaction to receive services from TOTAL VISION. She did so with
26 the understanding that TOTAL VISION would keep her PII secure. Had TOTAL
27 VISION disclosed to Ramey that her PII would not be kept secure and would be
28 kept in a manner easily accessible to hackers and third parties, she would have
taken additional precautions relating to her PII or would not have provided it to
TOTAL VISION. Ramey considered adequate data security to be a part of her

1 transactions with TOTAL VISION. Plaintiff Ramey has suffered the injuries due to
2 this Data Breach further set forth herein.

3 23. Plaintiff Jane Doe (or "Jane Doe") is and was at all times relevant to this
4 action a resident of the State of California and citizen of the State of California.
5 Plaintiff Jane Doe received a notice addressed to her, sent on TOTAL VISION's
6 behalf, entitled "*Important Security Notification*," dated December 4, 2020, signed
7 by Doug Cannon, Chief Financial Officer, for TOTAL VISION, stating, in part:

8 We are contacting you regarding a data security incident
9 that has occurred on October 30, 2020 at Total Vision, LLC.
10 This incident involved your name, address, date of birth,
11 social security number, and contact lens or eyeglass
12 prescription. . . . [¶] This information was located on a server
13 that was accessed by a third party. Upon learning of this
14 incident, we promptly secured the server and then
encrypted the information on the server. Our investigation
is ongoing at this time.

15 24. Prior to October 30, 2020, Jane Doe was a patient of, received medical
16 treatment and diagnosis from, and provided her PII to Defendant PACK AND
17 BIANES, Defendant John C. Pack, O.D., and Defendant Beverly BIANES, O.D.,
18 doing business as "Pack and BIANES Vision Care" and "Pack and BIANES Vision
19 Care Optometry," including her name, address, date of birth, social security
20 number, phone number and email address, as part of a transaction to receive
21 services from Defendants. She did so with the understanding that Defendants
22 would keep her PII secure. Had Defendants disclosed to Jane Doe that her PII
23 would not be kept secure and would be kept in a manner easily accessible to
24 hackers and third parties, she would have taken additional precautions relating to
25 her PII or would not have provided it to TOTAL VISION. Jane Doe considered
26 adequate data security to be a part of her transactions with TOTAL VISION.

1 **C. DOE Defendants**

2 25. The true names and capacities, whether individual, corporate, associate,
3 or otherwise, of defendants DOES 1 through 100, inclusive, are unknown to
4 Plaintiffs, who therefore sues said defendants by such fictitious names under the
5 Code of Civil Procedure § 474. Plaintiffs are informed and believe and thereon
6 allege that each of the defendants herein designated as a DOE is responsible in
7 some manner for the events herein referred to and caused injuries and damages as
8 alleged. Plaintiffs will seek leave of court and/or amend this complaint to reflect
9 the true names and capacities of the Defendants designated hereinafter as DOES 1
10 through 100 when such identities become known to Plaintiffs. Any reference
11 made to a named Defendant by specific name or otherwise, individually or plural,
12 is also a reference to the actions or inactions of DOES 1 through 100, inclusive.

13 26. Plaintiffs are informed and believe and thereon allege that at all times
14 herein mentioned each of the Defendants was the agent, servant and/or employee
15 of the remaining Defendants, and at all times herein mentioned, each was acting
16 with the time, place and scope of said agency and employment.

17 27. At all times herein mentioned, Defendants were acting as the ostensible
18 agents of each and every other Defendant and were doing so at the behest of and
19 with the approval of said Defendants. At all times herein relevant, Plaintiffs
20 reasonably and without negligence relied on the representations made by all
21 Defendants about the agency and employment of the remaining Defendants to
22 Plaintiffs' detriment.

23 **JURISDICTION AND VENUE**

24 28. This Court has jurisdiction over this action under California Code of
25 Civil Procedure section 410.10. The aggregated amount of damages incurred by
26 Plaintiffs and the Class exceed the jurisdictional minimum of this Court.

29. The Court has personal jurisdiction over Defendants because their contacts with the State of California are systematic, continuous, and sufficient to subject it to personal jurisdiction in this Court.

30. Venue in this Court is appropriate under Code of Civil Procedure sections 395(a) and 395.5 because Defendant TOTAL VISION is a limited liability company with its principal place of business in California. Defendant PACK AND BIANES has its principal business office and registered agent of service of process in the County of San Diego. In addition, Plaintiffs reside in the County of San Diego, and a substantial portion of the events giving rise to this litigation happened in the County of San Diego.

FACTUAL ALLEGATIONS

A. Defendants collect and store thousands of patients' PII and fails to provide adequate data security for the PII.

31. As a part of its business and optometry operations, Defendants collect a variety of PII from their patients. On its website, TOTAL VISION represents that it has "Over 75 doctors with 35 locations" in California and that "Total Vision providers offer primary eye care services including prescription glasses, contact lenses, evaluation of ocular health, emergency visits, and LASIK consultations."⁸ The website also states, "Total Vision optometry offices provide world-class vision care. Our network of providers meet our standards for professionalism and quality, and offer advanced testing and treatment."⁹

32. Defendants are obligated by both California common law and a number of statutes, to implement reasonable and appropriate data security measures to keep the PII of its patients, including Plaintiffs, Class members, and Subclass members, secure.

⁸ (<https://yourtotalvision.com>, last visited April 21, 2021).

⁹ (<https://yourtotalvision.com/about/>, last visited April 22, 2021).

1 33. Unfortunately, Defendants did not implement reasonable and
2 appropriate data security measures and, as a result, on or about October 30, 2020,
3 an unknown third party gained access to a TOTAL VISION server that was used
4 to store Plaintiffs' and the Class's PII. At the time of the breach, the PII was
5 stored in an unencrypted format, in violation of both the law and basic data
6 safety protocols.

7 34. Among the information stolen from the server was Plaintiffs' and Class'
8 names, addresses, dates of birth, social security numbers, and prescription
9 information. This PII was the direct target of the data theft and was viewed by
10 the thieves.

11 35. All of the above incidents and the damages flowing from them were
12 directly and legally caused by Defendants' failure to implement and maintain
13 adequate data security as required by law.

14 **B. Defendants' collection and storage of patients' PII subjects Defendants to**
15 **statutory requirements.**

16 36. As providers of health care, contractors, and/or other recipient of
17 medical information, Defendants are required by the CMIA to ensure that medical
18 information regarding a patient is not disclosed or disseminated or released
19 without their patients' authorization, and to protect and preserve the
20 confidentiality of the medical information regarding a patient, under Civil Code
21 §§ 56.10, 56.26, 56.36, and 56.101.

22 37. As providers of health care, contractors, and/or other recipient of
23 medical information, Defendants are required by the CMIA to:

- 24 a. not disclose medical information regarding a patient without first
25 obtaining an authorization under Civil Code §§ 56.10 and 56.26;
26 b. create, maintain, preserve, and store medical information in a manner
27 that preserves the confidentiality of the information contained therein
28 under Civil Code § 56.101(a);

- 1 c. protect and preserve confidentiality of electronic medical information
2 of Plaintiffs, the Class, and the SubClass in its possession under Civil
3 Code § 56.101(b)(1)(A);
- 4 d. take appropriate preventive actions to protect the confidential
5 information or records against release consistent with Defendants'
6 obligations under the CMIA, under Civil Code § 56.36(e)(2)(E), or other
7 applicable state law, and the Health Insurance Portability and
8 Accountability Act of 1996 (Public Law 104-191) (HIPAA) and all
9 HIPAA Administrative Simplification Regulations in effect on January
10 1, 2012, contained in Parts 160, 162, and 164 of Title 45 of the Code of
11 Federal Regulations, and Part 2 of Title 42 of the Code of Federal
12 Regulations, including, but not limited to, all of the following:
- 13 i. developing and implementing security policies and procedures;
 - 14 ii. designating a security official who is responsible for developing
15 and implementing its security policies and procedures, including
16 educating and training the workforce; and
 - 17 iii. encrypting the information or records, and protecting against the
18 release or use of the encryption key and passwords, or
19 transmitting the information or records in a manner designed to
20 provide equal or greater protections against improper
21 disclosures.

22 38. By law, the HIPAA Privacy Rule applies only to covered entities, e.g.
23 health care providers. However, most health care providers do not carry out all of
24 their health care activities and functions by themselves. Instead, they often use the
25 services of a variety of other persons or businesses. The Privacy Rule allows
26 covered providers to disclose protected health information to these "business
27 associates" if the providers obtain assurances that the business associate will use
28 the information only for the purposes for which it was engaged by the covered

entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule.

39. Covered entities may disclose protected health information to an entity in its role as a business associate only to help the covered entity carry out its health care functions – not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate. The Privacy Rule requires that a covered entity obtain assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.

40. Alternatively, Plaintiff Jane Doe alleges on information and belief that PACK AND BIANES's, Defendant John C. Pack, O.D.'s, and Defendant Beverly BIANES, O.D.'s disclosure of and/or delivery of Plaintiff Jane Doe's and the SubClass members' medical information to TOTAL VISION was without a business associate agreement or pursuant to a business associate agreement that was not permissible under the Privacy Rule or any exemption under Civil Code § 56.10(c), and/or because PACK AND BIANES, Defendant John C. Pack, O.D., and Defendant Beverly BIANES, O.D., negligently failed to obtain reasonable assurances and conduct assessments of TOTAL VISION to verify that TOTAL VISION would comply with HIPAA privacy regulations and to follow guidelines and policies to maintain the privacy, confidentiality, including by encryption, and otherwise reasonably protect Plaintiff Jane Doe's and the SubClass members' medical information from disclosure and/or release to unauthorized persons prior to and after PACK AND BIANES's, Defendant John C. Pack, O.D.'s, and Defendant Beverly BIANES, O.D.'s disclosure of and/or delivery of Plaintiff Jane Doe's and the SubClass members' medical information to TOTAL VISION.

1 41. Based upon the information posted on the U.S. Department of Health
2 and Human Services' official website, TOTAL VISION reported on "12/28/2020"
3 a "Hacking/IT Incident" involving "Network Server" affecting "138,402" persons,
4 which involved a "Business Associate," to the U.S. Department of Health &
5 Human Services' Office for Civil Rights.

6 42. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires
7 HIPAA covered entities to provide notification following a breach of unsecured
8 protected health information. Following a breach of unsecured protected health
9 information, covered entities must provide notification of the breach to affected
10 individuals. Covered entities must *only* provide the required notifications if the
11 breach involved unsecured protected health information. Unsecured protected
12 health information – which is part of the PII at issue in this matter – is protected
13 health information that has not been rendered unusable, unreadable, or
14 indecipherable to unauthorized persons through the use of a technology or
15 methodology specified by the Secretary of the U.S. Department of Health and
16 Human Services in guidance. Under approved guidance of the U.S. Department
17 of Health and Human Services, protected health information is rendered unusable,
18 unreadable, or indecipherable to unauthorized individuals if (1) electronic
19 protected health information has been encrypted as specified in the HIPAA
20 Security Rule by "the use of an algorithmic process to transform data into a form
21 in which there is a low probability of assigning meaning without use of a
22 confidential process or key" (45 CFR 164.304 definition of encryption) and (2) such
23 confidential process or key that might enable decryption has not been
24 breached. By reporting this incident to the U.S. Department of Health and Human
25 Services, TOTAL VISION has determined and is affirming that the Class'
26 electronic PII was either not encrypted at all, or if it was encrypted, the encryption
27 has been breached by the unauthorized third party. As a result, Defendants were
28 negligent for failing to encrypt or adequately encrypt Plaintiffs' and Class

members' PII on their computer networks. Further, because Plaintiffs' and Class members' PII on Defendants' computer networks was not rendered unusable, unreadable, or indecipherable, the unauthorized third party or parties who accessed Plaintiffs' and Class members' PII was able to and did view Plaintiffs' and Class members' PII contained within TOTAL VISION's computer server.

43. At all times relevant to this action, including the period of before and on October 30, 2020, Defendants negligently created, maintained, preserved, and/or stored Plaintiffs' and Class members' PII, including their names, addresses, dates of birth, social security numbers, and contact lens or eyeglass prescriptions, in electronic form, on Defendants' computer networks in a manner that did not preserve the confidentiality of the information, and negligently failed to protect and preserve confidentiality of Plaintiffs' and Class members' PII in Defendants' possession, as required by HIPPA and the CMIA, and specifically, under Civil Code §§ 56.10(a), 56.26(a), 56.36(e)(2)(E), 56.101(a), and 56.101(b)(1)(A), and according to Defendants' written representations to Plaintiffs and Class members.

44. Had Defendants taken such appropriate preventive actions, fix the deficiencies in their data security systems and adopted security measures as required by HIPPA and the CMIA before and on October 30, 2020, Defendants could have prevented the Data Breach and Plaintiffs' and Class members' PII within Defendants' computer networks from being accessed and viewed by unauthorized third parties.

C. The PII exposed by Defendants as a result of their inadequate data security is highly valuable on the black market.

45. The information exposed by Defendants is a virtual goldmine for phishers, hackers, identity thieves and cyber criminals.

46. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law

1 enforcement has difficulty policing the “dark web” due to this encryption, which
2 allows users and criminals to conceal identities and online activity.

3 47. The PII of consumers remains of high value to criminals, as evidenced
4 by the prices they will pay through the dark web. Numerous sources cite dark web
5 pricing for stolen identity credentials. For example, personal information can be
6 sold at a price ranging from \$40 to \$200¹⁰.

7 48. Social Security numbers are among the worst kind of personal
8 information to have stolen because they may be put to a variety of fraudulent uses
9 and are difficult for an individual to change. The Social Security Administration
10 stresses that the loss of an individual’s Social Security number, as is the case here,
11 can lead to identity theft and extensive financial fraud:

12 A dishonest person who has your Social Security number
13 can use it to get other personal information about you.
14 Identity thieves can use your number and your good
15 credit to apply for more credit in your name. Then, they use
16 the credit cards and don’t pay the bills, it damages your
17 credit. You may not find out that someone is using your
18 number until you’re turned down for credit, or you begin to
19 get calls from unknown creditors demanding payment for
items you never bought. Someone illegally using your Social
Security number and assuming your identity can cause a lot
of problems.¹¹

20 49. What’s more, it is no easy task to change or cancel a stolen Social
21 Security number. An individual cannot obtain a new Social Security number
22 without significant paperwork and evidence of actual misuse. In other words,
23 preventive action to defend against the possibility of misuse of a Social Security
24

25
26 ¹⁰ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends,
27 Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed Nov. 11, 2020).

28 ¹¹ Social Security Administration, *Identity Theft and Your Social Security Number*, available at:
<https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Nov. 11, 2020).

1 number is not permitted; an individual must show evidence of actual, ongoing
2 fraud activity to obtain a new number.

3 50. Even then, a new Social Security number may not be effective.
4 According to Julie Ferguson of the Identity Theft Resource Center, "The credit
5 bureaus and banks are able to link the new number very quickly to the old
6 number, so all of that old bad information is quickly inherited into the new Social
7 Security number."¹²

8 51. Medical data is also especially valuable to identity thieves. According
9 to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a \$50 street
10 value" ¹³ In fact, the medical industry has experienced disproportionately
11 higher instances of data theft than any other industry.

12 52. Medical identity theft is one of the forms of identity theft that is most
13 common, most expensive, and most difficult to prevent. According to Kaiser
14 Health News, "medical-related identity theft accounted for 43 percent of all
15 identity thefts reported in the United States in 2013," which is more "than identity
16 thefts involving banking and finance, the government and the military, or
17 education."¹⁴

18 53. As indicated by Jim Trainor, second in command at the FBI's cyber
19 security division: "Medical records are a gold mine for criminals – they can access
20 a patient's name, DOB, Social Security and insurance numbers, and even financial
21 information all in one place."¹⁵

22
23 ¹² Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR
24 (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Nov. 11, 2020).

25 ¹³ Study: Few Aware of Medical Identity Theft Risk, Claims Journal,
26 <https://www.claimsjournal.com/news/national/2012/06/14/208510.htm> (last visited
27 Oct. 30, 2020).

28 ¹⁴ Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News,
Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/> (last visited Oct. 30, 2020).

¹⁵ IDExperts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, New
Ponemon Study Shows, <https://www.idexpertscorp.com/knowledge-center/single/you->

1 54. Because of this, the information compromised in the Data Breach here is
2 more valuable than the loss of, for example, credit card information in a retailer
3 data breach. There, victims can cancel or close credit and debit card accounts.
4 Here, the information compromised in this Data Breach – Social Security number,
5 prescription information, name, date of birth, and addresses – is impossible to
6 “close” and difficult, if not impossible, to change.

7 55. This data commands a much higher price on the black market. Martin
8 Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to
9 credit card information, personally identifiable information and Social Security
10 numbers are worth more than 10 times on the black market.”¹⁶

11 56. Once PII is sold, it is often used to gain access to various areas of the
12 victim’s digital life, including bank accounts, social media, credit card, and tax
13 details, as happened here. This can lead to additional PII being harvested from the
14 victim, as well as PII from family, friends, and colleagues of the original victim.

15 57. According to the FBI’s Internet Crime Complaint Center (IC3) 2019
16 Internet Crime Report, Internet-enabled crimes reached their highest number of
17 complaints and dollar losses in 2019, resulting in more than \$3.5 billion in losses to
18 individuals and business victims.

19 **D. Defendants were on notice of data breach threats and the inadequacy of**
20 **its security.**

21 58. Defendants were on notice that companies in the healthcare industry
22 are targets for cyberattacks.

23 59. In August 2014, after a cyberattack on Community Health Systems, Inc.,
24 the FBI warned companies within the healthcare industry that hackers were

25 got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited Oct.
26 30, 2020).

27 ¹⁶ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*
28 *Numbers*, IT World, (Feb. 6, 2015), available at:
<https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Nov. 11, 2020).

1 targeting them. The warning stated “[t]he FBI has observed malicious actors
2 targeting healthcare related systems, perhaps for the purpose of obtaining the
3 Protected Healthcare Information (PHI) and/or Personally Identifiable
4 Information (PII).”¹⁷

5 60. The California Data Breach Report 2012-2015, issued in February 2016
6 by Attorney General, Kamala D. Harris, reported, “Malware and hacking
7 presents the greatest threat, both in the number of breaches and the number of
8 records breached” and “Social Security numbers and medical information – was
9 breached than other data types.” Moreover, as Attorney General further reported,
10 just because

11 [e]xternal adversaries cause most data breaches, [] this does
12 not mean that organizations are solely victims; they are also
13 stewards of the data they collect and maintain. People
14 entrust businesses and other organizations with their data
15 on the understanding that the organizations have a both an
16 ethical and a legal obligation to protect it from unauthorized
17 access. Neglecting to secure systems and data opens a
gateway for attackers, who take advantage of uncontrolled
vulnerabilities.

18 61. Regarding encryption, Attorney General instructed in the California
19 Data Breach Report 2012-2015,

20 As we have said in the past, breaches of this type are
21 preventable. Affordable solutions are widely available:
22 strong full-disk encryption on portable devices and desktop
23 computers when not in use.[] Even small businesses that
24 lack full time information security and IT staff can do this.
25 They owe it to their patients, customers, and employees to
do it now.

26 ¹⁷ Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug.
27 2014), [https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-](https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820)
28 [healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820](https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820) (last visited
Oct. 30, 2020).

1 62. More recently the HIPAA Journal posted on November 1, 2018 warned,
2 “Healthcare organization[s] need to ensure that their systems are well protected
3 against cyberattacks, which means investing in technologies to secure the network
4 perimeter, detect intrusions, and block malware and phishing threats.”

5 63. The American Medical Association (“AMA”) also warned healthcare
6 companies about the importance of protecting their patients’ confidential
7 information:

8 Cybersecurity is not just a technical issue; it’s a patient safety
9 issue. AMA research has revealed that 83% of physicians
10 work in a practice that has experienced some kind of
11 cyberattack. Unfortunately, practices are learning that
12 cyberattacks not only threaten the privacy and security of
patients’ health and financial information, but also patient
access to care.¹⁸

13 64. Defendants were on notice that the healthcare industry as well as
14 federal and state governments had concerns about healthcare company data
15 encryption. Defendants knew they kept protected health and personal information
16 in their computer systems and yet did not encrypt its computer systems.

17 65. The United States Department of Health and Human Services’ Office
18 for Civil Rights urges the use of encryption of data containing sensitive personal
19 information. As long ago as 2014, the Department fined two healthcare companies
20 approximately two million dollars for failing to encrypt laptops containing
21 sensitive personal information. In announcing the fines, Susan McAndrew, the
22 DHHS’s Office of Human Rights’ deputy director of health information privacy,
23
24
25

26 ¹⁸ Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med.
27 Ass’n (Oct. 4, 2019), [https://www.ama-assn.org/practice-](https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals)
28 [management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-](https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals)
hospitals (last visited Oct. 30, 2020).

1 stated “[o]ur message to these organizations is simple: encryption is your best
2 defense against these incidents.”¹⁹

3 **E. Plaintiffs and Class Members are at increased risk of identity fraud.**

4 66. As a result of the Data Breach, Plaintiffs are and will continue to be at
5 heightened risk for financial fraud, identity theft, other forms of fraud, and the
6 attendant damages, for years to come.

7 67. As a result of Defendant’s failures to prevent the Data Breach,
8 Plaintiffs and Class members have suffered, will suffer, and are at increased risk
9 of suffering:

- 10 a. The compromise, publication, theft, and/or unauthorized use of
11 their PII;
- 12 b. Out-of-pocket costs associated with the prevention, detection, recovery,
13 and remediation from identity theft or fraud;
- 14 c. Lost opportunity costs and lost wages associated with efforts expended
15 and the loss of productivity from addressing and attempting to
16 mitigate the actual and future consequences of the Data Breach,
17 including but not limited to efforts spent researching how to prevent,
18 detect, contest, and recover from identity theft and fraud;
- 19 d. The continued risk to their PII, which remains in Defendants’
20 possession and is subject to further breaches so long as Defendants fail
21 to undertake appropriate measures to protect the PII in their
22 possession; and
- 23 e. Current and future costs in terms of time, effort, and money that will be
24 expended to prevent, detect, contest, remediate, and repair the impact
25

26 ¹⁹ *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. Dep’t of Health and Human
27 Services (Apr. 22, 2014), available at [https://wayback.archive-
28 it.org/3926/20150618190135/http://www.hhs.gov/news/press/2014pres/04/20140422
b.html](https://wayback.archive-it.org/3926/20150618190135/http://www.hhs.gov/news/press/2014pres/04/20140422b.html) (last visited Oct. 30, 2020).

1 of the Data Breach for the remainder of the lives of Plaintiffs and the
2 Class members.

3 68. In addition to a remedy for the economic harm, Plaintiffs and Class
4 members maintain an undeniable interest in ensuring that their PII is secure,
5 remains secure, and is not subject to further misappropriation and theft.

6 69. To date, other than providing 12 months of credit monitoring and
7 identity protection services, Defendants do not appear to be taking any measures
8 to assist Plaintiffs and Class members.

9 **CLASS ACTION ALLEGATIONS**

10 70. Pursuant to California Code of Civil Procedure Section 382, Plaintiffs
11 bring this action on behalf of themselves and the following proposed class, defined
12 as follows:

13 All persons residing in the State of California who had their PII
14 compromised as a result of the Data Breach that occurred on or
15 about October 30, 2020. [the "Class"]

16 71. Pursuant to California Code of Civil Procedure Section 382, Plaintiff
17 Jane Doe brings this action on behalf of herself and the following proposed
18 SubClass, defined as follows:

19 All persons residing in the State of California who were patients
20 of Defendant John C. Pack, O.D. and Beverly BIANES, O.D., Inc.,
21 Defendant John C. Pack, O.D., and/or Defendant Beverly BIANES,
22 O.D., doing business as "Pack and BIANES Vision Care" and/or
23 "Pack and BIANES Vision Care Optometry," and had their PII
24 compromised as a result of the Data Breach that occurred on or
about October 30, 2020. [the "SubClass"]

25 72. Excluded from the proposed Class are any officer or director of
26 Defendants; any officer or director of any affiliate, parent, or subsidiary of TOTAL
27 VISION or PACK AND BIANES; and any judge to whom this case is assigned, his
28 or her spouse, and members of the judge's staff.

1 73. Plaintiffs reserve the right under California Rule of Court 3.765 to
2 amend or modify the Class definition with greater particularity or further division
3 into subclasses or limitation to particular issues as warranted, and as additional
4 facts are discovery by Plaintiffs during their future investigations.

5 74. **Numerosity.** While the exact number of Class members, including the
6 members of the Subclass, is unknown to Plaintiffs at this time, Plaintiffs believe the
7 number of Class members is in the thousands. Members of the proposed Class and
8 SubClass are thus too numerous to practically join in a single action. Membership
9 in the Class and SubClass are readily ascertainable from Defendants' own records.

10 75. **Commonality and Predominance.** Common questions of law and fact
11 exist as to all proposed Class and SubClass members and predominate over
12 questions affecting only individual Class and SubClass members. These common
13 questions include:

- 14 a. Whether Defendants engaged in the wrongful conduct alleged herein;
- 15 b. Whether Defendants' inadequate data security measures were a cause
16 of the data security breach;
- 17 c. Whether Defendants owed a legal duty to Plaintiffs, Class members,
18 and/or SubClass members to exercise due care in collecting, storing,
19 and safeguarding their PII;
- 20 d. Whether Defendants negligently or recklessly breached legal duties
21 owed to Plaintiffs, Class members, and/or SubClass members to
22 exercise due care in collecting, storing, and safeguarding their PII;
- 23 e. Whether Plaintiffs, Class members, and/or SubClass members are at an
24 increased risk for identity theft because of the data security breach;
- 25 f. Whether Defendants' conduct violated California Business and
26 Professions Code section 17200 *et seq.*;
- 27 g. Whether Defendants failed to "implement and maintain reasonable
28 security procedures and practices" for Plaintiffs', Class members' and/

SubClass members' PII, in violation of California Civil Code section 1798.81.5, subdivision (b);

- h. Whether Defendants violated their duty to maintain and implement reasonable security procedures and practices resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiffs', Class members', and/or SubClass members' unredacted and unencrypted PII, in violation of California Civil Code section 1798.150;
- i. Whether Plaintiffs, Class members, and/or SubClass members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and
- j. Whether Plaintiffs, Class members, and/or SubClass members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

76. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the Class and SubClass members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

77. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class and SubClass. All Class and SubClass members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties.

78. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class and SubClass because their interests do not conflict with the interests of the other Class and SubClass members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and

1 Plaintiffs will prosecute this action vigorously. The interests of the Class and the
2 SubClass will be fairly and adequately protected by Plaintiffs and their counsel.

3 **79. Superiority:** A class action is superior to any other available means for
4 the fair and efficient adjudication of this controversy, and no unusual difficulties
5 are likely to be encountered in the management of this matter as a class action. The
6 damages, harm, or other financial detriment suffered individually by Plaintiffs,
7 Class members, and SubClass members are relatively small compared to the
8 burden and expense that would be required to litigate their claims on an
9 individual basis against Defendants, making it impracticable for Class members
10 and SubClass members to individually seek redress for Defendants' wrongful
11 conduct. Even if Class and SubClass members could afford individual litigation,
12 the court system could not. Individualized litigation would create a potential for
13 inconsistent or contradictory judgments and increase the delay and expense to all
14 parties and the court system. By contrast, the class action device presents far fewer
15 management difficulties and provides the benefits of single adjudication,
16 economies of scale, and comprehensive supervision by a single court.

17 **FIRST CAUSE OF ACTION**

18 **Violation of the California's Unfair Competition Law**

19 **Cal. Bus. & Prof. Code § 17200, *et seq.***

20 **(On behalf of Plaintiffs, the Class, and the SubClass Against all Defendants)**

21 **80.** Plaintiffs incorporate by reference all previous allegations as though
22 fully set forth herein.

23 **81.** By reason of the conduct alleged herein, Defendants engaged in
24 unlawful and/or unfair business practices as defined in California's Unfair
25 Competition Law ("UCL"), Business and Professions Code § 17200 *et seq.*

26 **82.** By reason of the conduct alleged herein, Defendants engaged in
27 "unlawful" business acts and practices in violation of the aforementioned statutes,
28 including Civil Code §§ 56.10(a), 56.26(a), 56.36(e)(2)(E), 56.101(a), 56.101(b)(1)(A),

1798.82(a) and 1798.82(d). Plaintiffs reserve the right to allege other violations of law committed by Defendants that constitute unlawful acts or practices within the meaning of California Business & Professions Code §§ 17200, *et seq.*

83. By reason of the conduct alleged herein, Defendants also engaged in “unfair” business acts or practices in that the harm caused by Defendants’ failure to maintain adequate information security procedures and practices, including but not limited to:

- a. failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions, failing to properly and adequately educate and train its employees,
- b. failing to put into place reasonable or adequately computer systems and security practices to safeguard patients’ identifiable medical information including access restrictions and encryption,
- c. failing to have adequate privacy policies and procedures in place that did not preserve the confidentiality of the medical and personal identifying information of Plaintiffs, the Class, and the SubClass in their possession, and
- d. failing to protect and preserve confidentiality of electronic medical information of Plaintiffs, the Class, and the SubClass in their possession against disclosure and/or release.

84. These failures outweigh the utility of such conduct and such conduct offends public policy, is immoral, unscrupulous, unethical, deceitful and offensive, and causes substantial injury to Plaintiffs, the Class, and the SubClass.

85. Plaintiffs and Class members suffered injury in fact, and lost money or property as the result of Defendants’ unlawful business practices. Defendants have obtained money and property from Plaintiffs, the Class, and the SubClass because of the payment of the services and products they received from Defendants. Plaintiffs, the Class, and the SubClass have suffered injury in fact by acquiring

1 less in their transactions with Defendants for the services and products they
2 received from Defendants than they otherwise would have if Defendants would
3 had adequately protected the confidentiality of their medical and personal
4 identifying information.

5 86. Further, Plaintiff Ramey spent time and money remedying the effects of
6 the Data Breach and did not receive the benefit of her bargain with Defendant
7 Total Vision, in that the services she received and paid for should have included
8 keeping her PII encrypted and secure – but did not.

9 87. In addition, Plaintiffs’ and all Class members’ PII was taken and is in
10 the hands of those who will use it for their own advantage, or is being sold for
11 value, making it clear that the hacked information is of tangible value.

12 88. The harm caused by Defendants’ actions and omissions, as described in
13 detail above, greatly outweigh any perceived utility. Indeed, Defendants’ failure to
14 follow basic data security protocols and misrepresentations or omissions to
15 Plaintiffs and Class members about Defendants’ data security cannot be said to
16 have had any utility at all. These actions and omissions were clearly injurious to
17 Plaintiffs and all Class members, directly causing the harms alleged below.

18 89. Defendant’s actions and omissions, as described in detail above,
19 violated fundamental public policies expressed by the California Legislature. See,
20 e.g., Cal. Civ. Code § 1798.1 (“The Legislature declares that . . . all individuals have
21 a right of privacy in information pertaining to them The increasing use of
22 computers . . . has greatly magnified the potential risk to individual privacy that
23 can occur from the maintenance of personal information.”); Cal. Civ. Code §
24 1798.81.5(a) (“It is the intent of the Legislature to ensure that personal information
25 about California residents is protected.”); Cal. Bus. & Prof. Code § 22578 (“It is the
26 intent of the Legislature that this chapter [including the Online Privacy Protection
27 Act] is a matter of statewide concern.”). Defendants’ acts and omissions thus
28 amount to a violation of the law.

1 90. The harm caused by Defendants' actions and omissions, as described in
2 detail above, is substantial in that it affects thousands of Class members and has
3 caused those persons to suffer actual harms. Such harms include a current and
4 ongoing substantial risk of identity theft, disclosure of Plaintiffs' and all Class
5 members' PII to third parties without their consent, loss of benefit of the bargain,
6 consequential out of pocket losses for procuring credit freeze or protection
7 services, identity theft monitoring, and other expenses relating to identity theft
8 losses or protective measures. This harm continues given the fact that Plaintiffs'
9 and all Class members' PII remains in Defendants' possession, without adequate
10 protection, and is also in the hands of those who obtained it without their consent.

11 91. As a result of Defendants' unlawful and/or unfair business practices in
12 violation of the UCL, Plaintiffs and Class members are entitled to equitable relief,
13 including restitution and injunctive relief.

14 92. Pursuant to the Business & Professions Code § 17203, Plaintiffs, the
15 Class, and the SubClass seek an order of this Court awarding Plaintiffs, the Class,
16 and the SubClass restitution of monies wrongfully acquired by Defendants in the
17 form of payments for services by means of such unlawful, fraudulent and/or
18 unfair business acts and practices, so as to restore any and all monies to Plaintiffs,
19 the Class, and the SubClass which were acquired and obtained by means of such
20 unlawful and unfair business acts and practices, which ill-gotten gains are still
21 retained by Defendants.

22 93. The aforementioned unlawful, fraudulent, and/or unfair business acts
23 or practices conducted by Defendants were committed in the past and continues to
24 this day. Defendants failed to acknowledge the wrongful nature of their actions.
25 Defendants have not corrected or publicly issued comprehensive corrective notices
26 to Plaintiffs, the Class, and the SubClass, and have not corrected or enacted
27 adequate privacy policies and procedures to protect and preserve confidentiality
28 of Plaintiffs', the Class', and the SubClass' PII in their possession.

1 94. Because of Defendants' aforementioned conduct, Plaintiffs, the Class,
2 and the SubClass have no other adequate remedy of law in that absent injunctive
3 relief from the Court, Defendants are likely to continue to injure Plaintiffs, the
4 Class, and the SubClass.

5 95. Pursuant to Business & Professions Code § 17203, Plaintiffs, the Class,
6 and the SubClass also seek an order of this Court for equitable and/or injunctive
7 relief in the form of an order a declaring (1) Defendants' existing data security
8 measures fail to comply with its contractual obligations and duties of care; and
9 (2) Defendants must implement and maintain reasonable security measures to
10 comply with its duties of care and adequately safeguard Plaintiffs' and Class
11 members' PII, including, but not limited to:

- 12 a. Requiring Defendants to protect, including through encryption, all data
13 collected, maintained, and analyzed through the course of its business
14 in accordance with all applicable regulations, industry standards, and
15 federal, state, or local laws;
- 16 b. Requiring Defendants to delete, destroy, and purge Plaintiffs and Class
17 Members PII unless Defendants can provide to the Court reasonable
18 justification for the retention and use of such information when
19 weighed against the privacy interests of Plaintiffs and Class Members;
- 20 c. Requiring Defendants to implement and maintain a comprehensive
21 Information Security Program designed to protect the confidentiality
22 and integrity of Plaintiffs' and Class Members' PII;
- 23 d. Prohibiting Defendants from maintaining Plaintiffs' and Class
24 members' PII on a cloud-based database;
- 25 e. Requiring Defendants to engage independent third-party security
26 auditors/penetration testers as well as internal security personnel to
27 conduct testing, including simulated attacks, penetration tests, and
28 audits on Defendants' systems on a periodic basis, and ordering

- 1 Defendants to promptly correct any problems or issues detected by
2 such third-party security auditors;
- 3 f. Requiring Defendants to engage independent third-party security
4 auditors and internal personnel to run automated security monitoring;
- 5 g. Requiring Defendants to audit, test, and train its security personnel
6 regarding any new or modified procedures;
- 7 h. Requiring Defendants to segment data by, among other things, creating
8 firewalls and access controls so that if one area of Defendants' network
9 is compromised, hackers cannot gain access to other portions of
10 Defendants' systems;
- 11 i. Requiring Defendants to conduct regular database scanning and
12 security checks;
- 13 j. Requiring Defendants to establish an information security training
14 program that includes at least annual information security training for
15 all employees, with additional training to be provided as appropriate
16 based upon the employees' respective responsibilities with handling
17 PII, as well as protecting Plaintiffs' and Class members' PII;
- 18 k. Requiring Defendants to routinely and continually conduct internal
19 training and education, and on an annual basis to inform internal
20 security personnel how to identify and contain a breach when it occurs
21 and what to do in response to a breach;
- 22 l. Requiring Defendants to implement a system of tests to assess its
23 respective employees' knowledge of the education programs discussed
24 in the preceding subparagraphs, as well as randomly and periodically
25 testing employees' compliance with Defendants' policies, programs,
26 and systems for protecting PII;
- 27 m. Requiring Defendants to implement, maintain, regularly review, and
28 revise as necessary a threat management program designed to

- 1 appropriately monitor Defendants' information networks for threats,
2 both internal and external, and assess whether monitoring tools are
3 appropriately configured, tested, and updated;
- 4 n. Requiring Defendants to meaningfully educate all Class members about
5 threats they face as a result of the loss of their PII to third parties, as
6 well as the steps affected individuals must take to protect themselves;
- 7 o. Requiring Defendants to implement logging and monitoring programs
8 sufficient to track traffic to and from Defendants' servers;
- 9 p. For a period of 10 years, appointing a qualified and independent third-
10 party assessor to conduct a System and Organization Controls
11 ("SOC") 2 Type 2 attestation on an annual basis to evaluate Defendants'
12 compliance with the terms of the Court's final judgment, to provide
13 such report to the Court and to counsel for the class, and to report any
14 deficiencies with compliance of the Court's final judgment;
- 15 q. Requiring Defendants to design, maintain, and test its computer
16 systems to ensure PII in their possession is adequately secured
17 and protected;
- 18 r. Requiring Defendants to disclose any future data breaches in a timely
19 and accurate manner;
- 20 s. Requiring Defendants to implement multi-factor authentication
21 requirements;
- 22 t. Requiring Defendants' employees to change their passwords on a
23 timely and regular basis, consistent with best practices; and
- 24 u. Requiring Defendants to provide lifetime credit monitoring and
25 identity theft repair services to Class Members.

26 96. Pursuant to Business & Professions Code § 17203, Plaintiffs, the Class,
27 and the SubClass further seek an order of this Court for equitable and/or
28

injunctive relief in the form of requiring Defendants to publicly issue comprehensive corrective notices.

97. Because this case is brought for the purposes of enforcing important rights affecting the public interest, Plaintiffs, the Class and the SubClass also seek the recovery of attorneys' fees and costs in prosecuting this action against Defendants under Code of Civil Procedure § 1021.5 and other applicable law.

SECOND CAUSE OF ACTION

Negligence

(On behalf of Plaintiffs, the Class, and the SubClass Against all Defendants)

98. Plaintiffs incorporate by reference all previous allegations as though fully set forth herein.

99. Defendants owed a duty to Plaintiffs, the Class, and the SubClass to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs', the Class', and the SubClass' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiffs', the Class', and the SubClass' PII in Defendants' possession was adequately secured and protected, and encrypting the PII.

100. Because Plaintiffs, the Class, and the SubClass are or were patients of Defendants and received medical and optometry services from Defendants, Defendants have a special relationship with Plaintiffs, the Class, and the SubClass.

101. Defendants owed a duty of care to Plaintiffs, the Class, and the SubClass to provide security, consistent with industry standards, to ensure that their systems and networks adequately protected the PII of their patients – including Plaintiffs, the Class, and the SubClass.

102. Defendants owed a duty of care to Plaintiffs, the Class, and the SubClass because they were foreseeable and probable victims of any inadequate data security practices. Defendants knew or should have known of the inherent

1 risks in collecting and storing the PII of its current and former patients and the
2 critical importance of adequately securing such information.

3 103. Plaintiffs, the Class, and the SubClass entrusted Defendants with their
4 PII with the understanding that Defendants would safeguard their information,
5 and Defendants were in a position to protect against the harm suffered by
6 Plaintiffs, the Class, and the SubClass as a result of the Data Breach.

7 104. Defendants' own conduct also created a foreseeable risk of harm to
8 Plaintiffs, the Class, and the SubClass. Defendants' misconduct included failing to
9 implement the systems, policies, and procedures necessary to prevent the Data
10 Breach and failing to encrypt the PII.

11 105. Defendants knew, or should have known, of the risks inherent in
12 collecting and storing unencrypted PII, and the importance of adequate security.
13 Defendants knew about—or should have been aware of—numerous,
14 well-publicized data breaches affecting businesses in California and the
15 United States.

16 106. Defendants breached their duties to Plaintiffs, the Class, and the
17 SubClass by failing to provide fair, reasonable, or adequate computer systems and
18 data security to safeguard the PII of Plaintiffs, the Class, and the SubClass.

19 107. Because Defendants knew that a breach of its systems would damage
20 thousands of current and former patients of Defendants, including Plaintiffs, the
21 Class, and the SubClass, Defendants had a duty to adequately protect their data
22 systems and the PII contained therein.

23 108. Defendants also had independent duties under the CMIA requiring
24 Defendants to reasonably safeguard Plaintiffs', the Class', and the SubClass' PII.

25 109. Through Defendants' acts and omissions, including Defendants' failure
26 to provide adequate security and its failure to protect Plaintiffs', the Class', and the
27 SubClass' PII from being foreseeably accessed, Defendants unlawfully breached
28 their duty to use reasonable care to adequately protect and secure the PII of

1 Plaintiffs, the Class members, and the SubClass members during the time it was
2 within Defendants' possession or control.

3 110. In engaging in the negligent acts and omissions as alleged herein,
4 which permitted an unknown third party to access a Defendants' server
5 containing current and former patient PII, Defendants violated the CMIA, Civil
6 Code §§ 56, *et seq.*, the CRA, Civ. Code § 1798.80, *et seq.*, and the Consumer Privacy
7 Act of 2018, Civ. Code § 1798.100, *et seq.*

8 111. Plaintiffs, the Class, and the SubClass are among the class of persons
9 those laws were designed to protect, and the injuries suffered by Plaintiffs and the
10 Class members are the type of injuries those laws were intended to prevent. As a
11 result, Defendants are negligent *per se*.

12 112. Neither Plaintiffs nor the other Class and SubClass members
13 contributed to the Data Breach as described in this Complaint.

14 113. As a direct and proximate cause of Defendants' conduct, Plaintiffs, the
15 Class, and the SubClass have suffered, and/or will suffer, injury and damages,
16 including but not limited to:

- 17 a. the loss of the benefit of their bargain with Defendant(s);
 - 18 b. the publication and/or theft of their PII;
 - 19 c. out-of-pocket expenses associated with the prevention, detection, and
20 recovery from identity theft, tax fraud, and/or unauthorized use of
21 their PII;
 - 22 d. lost opportunity costs associated with effort expended and the loss of
23 productivity addressing and attempting to mitigate the actual and
24 future consequences of the Data Breach, including but not limited to
25 efforts spent researching how to prevent, detect, contest and recover
26 from tax fraud and identity theft;
 - 27 e. costs associated with placing freezes on credit reports;
- 28

- 1 f. anxiety, emotional distress, loss of privacy, and other economic and
2 non-economic losses;
- 3 g. the continued risk to their PII, which remains in Defendants' possession
4 and is subject to further unauthorized disclosures so long as
5 Defendants fail to undertake appropriate and adequate measures to
6 protect the PII of employees and former employees in their continued
7 possession; and,
- 8 h. future costs in terms of time, effort and money that will be expended to
9 prevent, detect, contest, and repair the inevitable and continuing
10 consequences of compromised PII for the rest of their lives.

11 **THIRD CAUSE OF ACTION**

12 **Breach of Implied Contract**

13 **(On behalf of Plaintiffs, the Class and the SubClass Against all Defendants)**

14 114. Plaintiffs incorporate by reference all previous allegations as though
15 fully set forth herein.

16 115. Defendants offered optometry and other services to Plaintiffs, the Class,
17 and the SubClass in exchange for compensation and other benefits. Defendants
18 either required Plaintiffs, the Class, and the SubClass to provide their PII or
19 acquired their PII with the authorization of Plaintiffs, the Class, and the SubClass.

20 116. Implied in these exchanges was a promise by Defendants to ensure that
21 the PII of Plaintiffs, the Class, and the SubClass in its possession was only used to
22 provide the agreed-upon services and other benefits from Defendants.

23 117. Defendants were therefore required to reasonably safeguard and
24 protect the PII of Plaintiffs, the Class, and the SubClass from unauthorized
25 disclosure or use.

26 118. Plaintiffs, the Class, and the SubClass accepted Defendants' offer for
27 services and fully performed their obligations under the implied contract with
28

1 Defendants by providing payment, or causing payment to be made, and their PII,
2 directly or indirectly, to Defendants.

3 119. Plaintiffs, the Class, and the SubClass would not have provided and
4 entrusted their PII to Defendants in the absence of their implied contracts with
5 Defendants, and would have instead retained the opportunity to control their PII
6 for uses other than services from Defendants.

7 120. Defendants breached the implied contracts with Plaintiffs, the Class,
8 and the SubClass by failing to reasonably safeguard and protect Plaintiffs', the
9 Class', and the SubClass' PII.

10 121. As a proximate and direct result of Defendants' breaches of its implied
11 contracts with Plaintiffs, the Class, and the SubClass, Plaintiffs, the Class, and the
12 SubClass suffered economic damages as described in detail above.

13 **FOURTH CAUSE OF ACTION**

14 **Violation of the Confidentiality of Medical Information Act**
15 **Cal. Civ. Code § 56, *et seq.***
16 **(On behalf of Plaintiffs, the Class, and the SubClass**
17 **Against Defendant Total Vision, LLC)**

18 122. Plaintiffs incorporates by reference all previous allegations as though
19 fully set forth herein.

20 123. At all times relevant to this action, including the period on and before
21 October 30, 2020, Defendant TOTAL VISION is a "licensed health care provider"
22 or "provider of health care" as defined in Civil Code § 56.05, subds. (h) and (m), a
23 "contractor" under Civil Code § 56.05, subd. (d), and/or "engaged in the business
24 of furnishing administrative services to programs that provide payment for health
25 care services" under Civil Code § 56.26, subd. (a).

26 124. Defendant TOTAL VISION maintained and continues to maintain
27 "medical information" within the meaning of Civil Code § 56.05, subd. (j), of
28 Plaintiffs, the Class, and the SubClass.

1 125. Plaintiffs, the Class, and the SubClass are “patients,” of TOTAL VISION
2 or other Defendants or other providers of health care, as defined in Civil Code
3 section 56.05, subd. (k), on or before October 30, 2020.

4 126. Plaintiffs, the Class, and the SubClass are “endanger[ed]” within the
5 meaning of Civil Code § 56.05(e) because they fear that disclosure of their medical
6 information could subject them to harassment or abuse.

7 127. Furthermore, Plaintiffs, the Class, and the SubClass had their
8 individually identifiable “medical information,” within the meaning of Civil Code
9 § 56.05(j), including their names, addresses, dates of birth, social security numbers,
10 and contact lens or eyeglass prescriptions, in electronic form, created, maintained,
11 preserved, and stored on Defendant TOTAL VISION’s computer network in a
12 manner that did not preserve the confidentiality of the information, and
13 negligently failed to protect and preserve confidentiality of electronic medical
14 information of Plaintiffs, the Class, and the SubClass in its possession, as required
15 by the CMIA, and specifically, under Civil Code §§ 56.10(a), 56.26(a),
16 56.36(e)(2)(E), 56.101(a), and 56.101(b)(1)(A), and according to their written
17 representations to Plaintiff and the Class at all times relevant to this action,
18 including the period on or before October 30, 2020.

19 128. Defendant TOTAL VISION negligently created, maintained, preserved,
20 stored, and then disclosed Plaintiffs’, the Class’, and the SubClass’ “medical
21 information,” within the meaning of Civil Code § 56.05(j), including Plaintiffs’, the
22 Class’, and the SubClass’ names, addresses, dates of birth, social security numbers,
23 and prescription information in electronic form, to be accessed and viewed by at
24 least one unauthorized third party, without first obtaining an authorization, in
25 violation of Civil Code §§ 56.10(a) and 56.26(a).

26 129. Defendant TOTAL VISION negligently created, maintained, preserved,
27 stored, and released Plaintiffs’, the Class’, and the SubClass’ “medical
28 information,” within the meaning of Civil Code § 56.05(j), including Plaintiffs’, the

1 Class', and the SubClass' names, addresses, dates of birth, social security numbers,
2 and prescription information in electronic form, to be accessed and viewed by at
3 least one unauthorized third party, without first obtaining an authorization, in
4 violation of Civil Code § 56.101(a).

5 130. As a result of this negligence, Plaintiffs', the Class', and the SubClass'
6 information was accessed and viewed by at least one unauthorized third party in
7 the Data Breach.

8 131. As a result of Defendant TOTAL VISION's above-described conduct
9 in violation of the CMIA, Plaintiffs, the Class, and the SubClass have suffered
10 damages from the unauthorized disclosure and/or release of their medical and
11 personal identifying information made unlawful by Civil Code §§ 56.10, 56.26,
12 and 56.101.

13 132. Because the CMIA allows for the remedies and penalties provided
14 under Civil Code § 56.36(b) as a result of TOTAL VISION's above-described
15 conduct in violation of the CMIA, Plaintiffs, individually and for each member of
16 the Class and the SubClass, seek nominal damages of one thousand dollars
17 (\$1,000) for each violation under Civil Code §56.36(b)(1), and actual damages
18 suffered, according to proof, for each violation under Civil Code § 56.36(b)(2).

19 **FIFTH CAUSE OF ACTION**

20 **Violation of the Confidentiality of Medical Information Act**

21 **Cal. Civ. Code § 56, *et seq.***

22 **(On behalf of Plaintiff Jane Doe and the SubClass Against**
23 **Defendants John C. Pack, O.D. and Beverly Bianes, O.D., Inc.,**
John C. Pack, O.D., and Beverly Bianes, O.D.)

24 133. Plaintiffs incorporate by reference all previous allegations as though
25 fully set forth herein.

26 134. At all times relevant to this action, including the period of before and
27 on October 30, 2020, PACK AND BIANES, John C. Pack, O.D., and Beverly Bianes,
28 O.D. are each a "licensed health care provider" or "provider of health care" as

1 defined in Civil Code section 56.05, subds. (h) and (m), and maintained and
2 continue to maintain “medical information” within the meaning of Civil Code
3 § 56.05(j), of Plaintiff Jane Doe and the SubClass.

4 135. Plaintiff Jane Doe and the SubClass are “patients” of PACK AND
5 BIANES, John C. Pack, O.D., and Beverly Bianes, O.D. or other Defendants within
6 the meaning of Civil Code § 56.05(k) and are “endanger” within the meaning of
7 Civil Code § 56.05(e) because they fear that disclosure and/or release of their
8 medical information could subject them to harassment or abuse.

9 136. At all times relevant to this action, including the period of before and
10 on October 30, 2020, PACK AND BIANES, John C. Pack, O.D., and Beverly Bianes,
11 O.D. negligently created, maintained, preserved, and/or stored Plaintiff Jane
12 Doe’s and the SubClass’ medical information, including their names, addresses,
13 dates of birth, social security numbers, and prescriptions, in electronic form, onto
14 Defendants’ computer networks in a manner that did not preserve the
15 confidentiality of the information, and negligently failed to protect and preserve
16 confidentiality of electronic medical information of Plaintiff Jane Doe and the
17 SubClass in their possession, as required by the CMIA, and specifically, under
18 Civil Code §§ 56.10(a), 56.101(a), 56.101(b)(1)(A), and 56.36(e)(2)(E), and according
19 to their written representations to Plaintiff Jane Doe and the SubClass.

20 137. Due to PACK AND BIANES’s, John C. Pack, O.D.’s, and Beverly
21 Bianes, O.D.’s disclosure and/or delivery of Plaintiff Jane Doe’s and the SubClass
22 members’ medical and personal identifying information to TOTAL VISION
23 without written authorization from Plaintiff Jane Doe and the SubClass or under
24 any exemption under Civil Code § 56.10(c), PACK AND BIANES, John C. Pack,
25 O.D., and Beverly Bianes, O.D. allowed Plaintiff Jane Doe’s and the SubClass’
26 medical information, including their names, addresses, dates of birth, social
27 security numbers, and prescriptions, in electronic form, to be accessed and viewed
28

1 by at least one unauthorized third party, without first obtaining an authorization,
2 constituting a disclosure in violation of Civil Code § 56.10(a).

3 138. Due to PACK AND BIANES's, John C. Pack, O.D.'s, and Beverly
4 Bianes, O.D.'s negligent creation, maintenance, preservation and/or storage of
5 Plaintiff Jane Doe's and the SubClass members' medical information on TOTAL
6 VISION's computer server, PACK AND BIANES, John C. Pack, O.D., and Beverly
7 Bianes, O.D. allowed Plaintiff Jane Doe's and the SubClass' medical information,
8 including their names, addresses, dates of birth, social security numbers, and
9 prescriptions, in electronic form, to be accessed and viewed by at least one
10 unauthorized third party, without first obtaining an authorization, constituting a
11 disclosure in violation of Civil Code § 56.10(a).

12 139. Due to PACK AND BIANES's, John C. Pack, O.D.'s, and Beverly
13 Bianes, O.D.'s disclosure and/or delivery Plaintiff Jane Doe's and the SubClass
14 members' medical and personal identifying information to TOTAL VISION
15 without written authorization from Plaintiff Jane Doe and the SubClass or under
16 any exemption under Civil Code § 56.10(c), PACK AND BIANES, John C. Pack,
17 O.D., and Beverly Bianes, O.D. allowed Plaintiff Jane Doe's and the SubClass'
18 medical information, including their names, addresses, dates of birth, social
19 security numbers, and prescriptions, in electronic form, to be accessed and viewed
20 by at least one unauthorized third party, constituting a release in violation of Civil
21 Code § 56.101(a).

22 140. Due to PACK AND BIANES's, John C. Pack, O.D.'s, and Beverly
23 Bianes, O.D.'s negligent creation, maintenance, preservation and/or storage of
24 Plaintiff Jane Doe's and the SubClass members' medical information on TOTAL
25 VISION's computer server, PACK AND BIANES, John C. Pack, O.D., and Beverly
26 Bianes, O.D. allowed Plaintiff Jane Doe's and the SubClass' medical information,
27 including their names, addresses, dates of birth, social security numbers, and
28 prescriptions, in electronic form, to be accessed and viewed by at least one

1 unauthorized third party, constituting a release in violation of Civil Code
2 § 56.101(a).

3 141. Due to PACK AND BIANES's, John C. Pack, O.D.'s, and Beverly
4 Bianes, O.D.'s disclosure and/or delivery Plaintiff Jane Doe's and the SubClass'
5 medical information and personal identifying information to TOTAL VISION
6 without written authorization from Plaintiff Jane Doe and the SubClass or under
7 any exemption under Civil Code § 56.10(c), PACK AND BIANES, John C. Pack,
8 O.D., and Beverly Bianes, O.D. allowed Plaintiff Jane Doe's and the SubClass'
9 medical information, including their names, addresses, dates of birth, social
10 security numbers, and prescriptions, in electronic form, to be accessed and viewed
11 by at least one unauthorized third party, constituting a release in violation of Civil
12 Code § 56.101(b)(1)(A).

13 142. Due to the negligent creation, maintenance, preservation and/or
14 storage of Plaintiff Jane Doe's and the SubClass members' medical information on
15 TOTAL VISION's computer server, PACK AND BIANES, John C. Pack, O.D., and
16 Beverly Bianes, O.D. allowed Plaintiff Jane Doe's and the SubClass' medical
17 information, including their names, addresses, dates of birth, social security
18 numbers, and prescriptions, in electronic form, to be accessed and viewed by at
19 least one unauthorized third party, constituting a release in violation of Civil Code
20 § 56.101(b)(1)(A).

21 143. As a result of above-described conduct of PACK AND BIANES, John C.
22 Pack, O.D., and Beverly Bianes, O.D. in violation of the CMIA, Plaintiff Jane Doe
23 and the SubClass have suffered damages from the unauthorized disclosure and/or
24 release of their medical and personal identifying information made unlawful by
25 Civil Code §§ 56.10, 56.101.

26 144. As a result of above-described conduct of PACK AND BIANES, John C.
27 Pack, O.D., and Beverly Bianes, O.D. in violation of the CMIA, Plaintiff Jane Doe
28 and the SubClass seek nominal damages of one thousand dollars (\$1,000) for each

1 violation under Civil Code §56.36(b)(1), and actual damages suffered, according to
2 proof, for each violation under Civil Code § 56.36(b)(2).

3 **SIXTH CAUSE OF ACTION**

4 **Breach of California Security Notification Laws**

5 **Cal. Civil Code § 1798.82**

6 **(On Behalf of Plaintiffs, the Class, and the SubClass Against Defendants Total
7 Vision, LLC and John C. Pack, O.D. and Beverly Bienes, O.D., Inc.)**

8 145. Plaintiffs incorporate by reference all previous allegations as though
9 fully set forth herein.

10 146. Pursuant to Civil Code § 1798.82(a),

11 A person or business that conducts business in California,
12 and that owns or licenses computerized data that includes
13 personal information, shall disclose a breach of the security
14 of the system following discovery or notification of the
15 breach in the security of the data to a resident of California
16 (1) whose unencrypted personal information was, or is
17 reasonably believed to have been, acquired by an
18 unauthorized person, or, (2) whose encrypted personal
19 information was, or is reasonably believed to have been,
20 acquired by an unauthorized person and the encryption key
21 or security credential was, or is reasonably believed to have
22 been, acquired by an unauthorized person and the person
23 or business that owns or licenses the encrypted information
24 has a reasonable belief that the encryption key or security
25 credential could render that personal information readable
26 or usable. The disclosure shall be made in the most
27 expedient time possible and without unreasonable delay,
28 consistent with the legitimate needs of law enforcement, as
provided in subdivision (c), or any measures necessary to
determine the scope of the breach and restore the reasonable
integrity of the data system.

25 Prior to passages of such statute, the California State Assembly cited an incident
26 where authorities knew of the breach in security for 21 days “before state workers
27 were told” as an example of “late notice.”
28

1 147. Civil Code § 1798.82 further provides,

2 (h) For purposes of this section, 'personal information'
3 means an individual's first name or first initial and last
4 name in combination with any one or more of the following
5 data elements, when either the name or the data elements
6 are not encrypted: (1) Social security number. (2) Driver's
7 license number or California Identification Card number.
8 (3) Account number, credit or debit card number, in
9 combination with any required security code, access code,
10 or password that would permit access to an individual's
11 financial account. (4) Medical information. (5) Health
12 insurance information. (i) . . . (2) For purposes of this
13 section, 'medical information' means any information
14 regarding an individual's medical history, mental or
15 physical condition, or medical treatment or diagnosis by a
16 health care professional. (3) For purposes of this section,
17 'health insurance information' means an individual's health
18 insurance policy number or subscriber identification
19 number, any unique identifier used by a health insurer to
20 identify the individual, or any information in an
21 individual's application and claims history, including any
22 appeals records.

17 148. Defendant TOTAL VISION conducts business in California and owns
18 or licenses computerized data which includes the PII, within the meaning of Civil
19 Code § 1798.82(h), of Plaintiffs and the Class.

20 149. PACK AND BIANES conducts business in California and owns or
21 licenses computerized data which includes the personal information, within the
22 meaning of Civil Code § 1798.82(h), of Plaintiff Jane Doe and the SubClass.

23 150. Based upon Defendant TOTAL VISION's "**Important Security**
24 **Notification**" form letter referenced above, PACK AND BIANES was aware that
25 Plaintiff Jane Doe's and the SubClass' unencrypted personal information on
26 TOTAL VISION's computer server was, or is reasonably believed to have been,
27 acquired by an unauthorized person no later than October 30, 2020. Thereafter and
28 to date, PACK AND BIANES did not send notification letters to Plaintiff Jane Doe

1 and the SubClass. As a result, PACK AND BIANES's failure to provide any
2 notification letters to Plaintiff Jane Doe and the SubClass for at least 383 days after
3 it was aware that Plaintiff Jane Doe and the SubClass personal information was, or
4 was reasonably believed to have been, acquired by an unauthorized person, is
5 presumptively unreasonable notice in violation of Civil Code § 1798.82.

6 151. Based upon TOTAL VISION's "*Important Security Notification*" form
7 letter submitted to the Attorney General of the State of California and mailed to
8 Plaintiffs and the Class, TOTAL VISION was aware that Plaintiffs' and the Class'
9 unencrypted personal information on TOTAL VISION's computer server was, or
10 is reasonably believed to have been, acquired by an unauthorized person no later
11 than October 30, 2020, but did not begin to mail notification letters to Plaintiffs and
12 the Class until December 4, 2020. Thus, TOTAL VISION waited at least 35 days
13 before *beginning* to inform Plaintiffs and the Class of this incident and the
14 subsequent threat to Plaintiffs' and the Class' personal information.

15 152. As a result, TOTAL VISION did not disclose to Plaintiffs and the Class
16 that their personal information was, or was reasonably believed to have been,
17 acquired by an unauthorized person, in the most expedient time possible and
18 without reasonable delay in violation of Civil Code § 1798.82(a).

19 153. Given the example of the Legislature finding that a delay of 21 days to
20 be "late notice" under the statute, TOTAL VISION's delay of 35 days before
21 *beginning* to inform Plaintiffs and the Class that their personal information was, or
22 was reasonably believed to have been, acquired by an unauthorized person by
23 mailing TOTAL VISION's form letter to Plaintiffs and the Class is presumptively
24 unreasonable notice in violation of Civil Code § 1798.82(a).

25 154. Upon information and belief, Plaintiffs believe and allege that no law
26 enforcement agency has notified Defendants that the notification would impede a
27 criminal investigation justifying PACK AND BIANES's decision not to notify
28 Plaintiff Jane Doe and the SubClass at all, or justifying TOTAL VISION's decision

1 to wait 35 days *before beginning to mail* notification letters to Plaintiffs and the Class
2 *after* they knew Plaintiffs' and the Class' unencrypted personal information on
3 TOTAL VISION's computer server was, or was reasonably believed to have been,
4 acquired by an unauthorized person.

5 155. Upon information and belief, Plaintiff Jane Doe believes and alleges
6 there were no measures taken by TOTAL VISION and PACK AND BIANES to
7 determine the scope of the breach or to restore the reasonable integrity of the data
8 system which justifies PACK AND BIANES's decision not to notify Plaintiff Jane
9 Doe and the SubClass, or TOTAL VISION's decision to wait 35 days *before*
10 *beginning to mail* notification letters to Plaintiffs and the Class. Moreover, TOTAL
11 VISION's notification letters mailed to Plaintiffs and the Class fail to provide
12 (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range
13 within which the breach occurred in violation of Civil Code § 1798.82(d)(2)(C).

14 156. Plaintiffs, the Class, and the SubClass have been injured by the fact that
15 Defendants did not disclose that Plaintiffs', the Class', and the SubClass' PII was,
16 or was reasonably believed to have been, acquired by an unauthorized person in
17 the most expedient time possible and without reasonable delay in violation of
18 Civil Code § 1798.82(a). Defendants' delays in informing required by Civil Code
19 § 1798.82(a) and providing all of the information required by Civil Code
20 § 1798.82(d) to Plaintiffs, the Class, and the SubClass that their PII was, or was
21 reasonably believed to have been, acquired by an unauthorized person, have
22 prevented Plaintiffs, the Class, and the SubClass from taking timely steps to
23 protect their personal information from unauthorized use and/or identify theft.

24 157. Plaintiffs, the Class, and the SubClass seek recovery of their damages
25 pursuant to Civil Code § 1798.84(b) and injunctive relief pursuant to Civil Code
26 § 1798.84(e).

1 **PRAYER FOR RELIEF**

2 WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly
3 situated, respectfully requests that the Court enter an order:

- 4 a. Certifying the proposed Class and SubClass as requested herein;
- 5 b. Appointing Plaintiffs as Classes Representatives, Plaintiff Jane Doe as Class
6 Representative of the SubClass, and undersigned counsel as Class Counsel;
- 7 c. Finding that Defendants engaged in the unlawful conduct as alleged herein;
- 8 d. Enjoining Defendants' conduct and requiring Defendants to implement
9 proper data security policies and practices; specifically:
- 10 i. prohibiting Defendants from engaging in the wrongful and
11 unlawful acts described herein;
- 12 ii. requiring Defendants to protect, including through encryption, all
13 data collected through the course of its business in accordance with
14 all applicable regulations, industry standards, and federal, state or
15 local laws;
- 16 iii. requiring Defendants to delete, destroy, and purge the PII of
17 Plaintiffs and the Class members unless Defendants can provide to
18 the Court reasonable justification for the retention and use of such
19 information when weighed against the privacy interests of Plaintiffs
20 and the Class members;
- 21 iv. requiring Defendants to implement and maintain a comprehensive
22 Information Security Program designed to protect the confidentiality
23 and integrity of the personal identifying information of Plaintiffs'
24 and the Class members' PII;
- 25 v. prohibiting Defendants from maintaining Plaintiffs' and the Class
26 members' PII on a cloud-based database;
- 27 vi. requiring Defendants to engage independent third-party security
28 auditors/penetration testers as well as internal security personnel to

- 1 conduct testing, including simulated attacks, penetration tests, and
2 audits on Defendants' systems on a periodic basis, and ordering
3 Defendants to promptly correct any problems or issues detected by
4 such third-party security auditors;
- 5 vii. requiring Defendants to engage independent third-party
6 security auditors and internal personnel to run automated
7 security monitoring;
- 8 viii. requiring Defendants to audit, test, and train their security
9 personnel regarding any new or modified procedures;
- 10 ix. requiring Defendants to segment data by, among other things,
11 creating firewalls and access controls so that if one area of
12 Defendants' network is compromised, hackers cannot gain access to
13 other portions of Defendants' systems;
- 14 x. requiring Defendants to conduct regular database scanning and
15 securing checks;
- 16 xi. requiring Defendants to establish an information security training
17 program that includes at least annual information security training
18 for all employees, with additional training to be provided as
19 appropriate based upon the employees' respective responsibilities
20 with handling PII, as well as protecting the PII of Plaintiffs and the
21 Class members;
- 22 xii. requiring Defendants to routinely and continually conduct internal
23 training and education, and on an annual basis to inform internal
24 security personnel how to identify and contain a breach when it
25 occurs and what to do in response to a breach;
- 26 xiii. requiring Defendants to implement a system of tests to assess their
27 respective employees' knowledge of the education programs
28 discussed in the preceding subparagraphs, as well as randomly and

- 1 periodically testing employees' compliance with Defendants'
2 policies, programs, and systems for protecting PII;
- 3 xiv. requiring Defendants to implement, maintain, regularly review, and
4 revise as necessary a threat management program designed to
5 appropriately monitor Defendants' information networks for
6 threats, both internal and external and assess whether monitoring
7 tools are appropriately configured, tested, and updated;
- 8 xv. requiring Defendants to meaningfully educate all Class members
9 about the threats they face as a result of the loss of their confidential
10 PII to third parties, as well as the steps affected individuals must
11 take to protect themselves;
- 12 xvi. requiring Defendants to implement logging and monitoring
13 programs sufficient to track traffic to and from Defendants' servers;
- 14 xvii. for a period of 10 years, appointing a qualified and independent
15 third-party assessor to conduct a SOC 2 Type 2 attestation on an
16 annual basis to evaluate Defendants' compliance with the terms of
17 the Court's final judgment, to provide such report to the Court and
18 to counsel for the class, and to report any deficiencies with
19 compliance of the Court's final judgment;
- 20 xviii. requiring Defendants to design, maintain, and test its computer
21 systems to ensure that PII in their possession is adequately secured
22 and protected;
- 23 xix. requiring Defendants to disclose any future data breaches in a
24 timely and accurate manner;
- 25 xx. requiring Defendants to implement multi-factor authentication
26 requirements;
- 27 xxi. requiring Defendants' employees to change their passwords on a
28 timely and regular basis, consistent with best practices; and

- xxii. requiring Defendants to provide lifetime credit monitoring and identity theft repair services to Class members.
- e. Awarding Plaintiffs, Class members, and SubClass members damages, including statutory damages;
- f. Awarding Plaintiffs, Classes members, and SubClass members pre-judgment and post-judgment interest on all amounts awarded;
- g. Awarding Plaintiffs, the Class members, and SubClass members reasonable attorneys' fees, costs, and expenses; and
- h. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class and SubClass, hereby demands a trial by jury as to all matters so triable.

Dated: November 18, 2021

CASEY GERRY SCHENK
FRANCAVILLA BLATT & PENFIELD, LLP

/s/ Gayle M. Blatt
GAYLE M. BLATT
*Attorneys for Plaintiff ANJANETTE RAMEY
and the Class*

Dated: November 18, 2021

KEEGAN & BAKER, LLP

/s/ Patrick N. Keegan
PATRICK N. KEEGAN
*Attorneys for Plaintiff JANE DOE and the Class
and SubClass*

EXHIBIT A



TOTAL VISION®
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

EXHIBIT A

December 4, 2020



G0290-L01-0000001 T00017 P003 *****ALL FOR AADC 123
SAMPLE A SAMPLE - L01 ADULT WITH CODE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789



RE: Important Security Notification
Please read this entire letter.

Dear Sample A Sample,

We are contacting you regarding a data security incident that has occurred on October 30, 2020 at Total Vision, LLC. This incident involved your name, address, date of birth, social security number, and contact lens or eyeglass prescription. As a result, your personal information may have been potentially exposed to others. No other medical information or financial information was potentially exposed to the third party.

This information was located on a server that was accessed by a third party. Upon learning of this incident, we promptly secured the server and then encrypted the information on the server. Our investigation is ongoing at this time. Please be assured that we are taking steps necessary to address the incident.

What we are doing to protect your information:

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: February 28, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (844) 955-2743 by **February 28, 2021**. Be prepared to provide engagement number **DB24122** as proof of eligibility for the identity restoration services by Experian.

0000001



EXHIBIT A

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (844) 955-2743. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at (844) 955-2743.

Sincerely,



Doug Cannon
Chief Financial Officer

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.