Natalie A. Lyons (293026)
Vess A. Miller (278020)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
nlyons@cohenandmalad.com
vmiller@cohenandmalad.com

Lynn A. Toops*
Amina A. Thomas*
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

J. Gerard Stranch, IV*
Andrew E. Mize*
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel J. Strauss*
Raina Borelli*
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
(608) 237-1775
sam@turkestrauss.com
raina@turkestrauss.com

Counsel for Plaintiff and the Proposed Class

*To seek admission *pro hac vice*

SUPERIOR COURT FOR THE STATE OF CALIFORNIA
FOR THE COUNTY OF ORANGE

ERIC E. EUFUSIA, Individually, and on behalf of all others similarly situated,

Plaintiff

v.

MEDICAL EYE SERVICES, INC. d/b/a MESVISION

Defendant.

Case No. 30-2023-01369472-CU-CO-CXC

CLASS ACTION COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF BASED ON:
(1) Negligence
(2) Negligence *per se*
(3) Breach of Contract
(4) Unjust Enrichment
(5) Invasion of Privacy – Intrusion Upon Seclusion
(6) Breach of Fiduciary Duty
(7) Violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff, ERIC E. EUFUSIA ("Plaintiff"), brings this Class Action Complaint ("Complaint") against Defendant Medical Eye Services, Inc. d/b/a MESVision ("MESVision" or "Defendant") individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows.

NATURE OF THE ACTION

1. This action arises out of Defendant's failures to safeguard the confidential personal information, Personally Identifying Information[1] ("PII") of its plan members, including Plaintiff and the proposed Class Members, resulting in the unauthorized disclosure of that PII in a cyberattack in May 2023 (the "Data Breach") to MESVision's vendor, MOVEit.[2] The PII disclosed in the Data Breach included Plaintiff and Class Members' names, dates of birth, addresses, Social Security numbers, subscriber/Member IDs, policy numbers, group number, and claim numbers.[3]

2. Defendant MESVision is vision benefits provider and administrator headquartered in California.[4] MESVision "provides vision care plans directly to thousands of employer groups and millions of plan members nationwide for leading health care organizations, insurance carriers, and self-funded employer group[s]."[5]

3. As a condition of providing vision insurance benefit services, MESVision required

---

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] *See* Johnson Financial Group, Notice of Data Security Event, **(hereinafter "Data Breach Notice") attached as Exhibit A**.

[3] *Id.*

[4] https://www.mesvision.com/aboutUs (last visited Dec. 17, 2023).

[5] *Id.*

its plan members to provide it with their PII, including names, dates of birth, and addresses.

4. MESVision engaged MOVEit, a third-party vendor, for its "secure file-transfer program" services.[6]

5. Unbeknownst to Plaintiff and the proposed Class Members, Defendant provided their PII to MOVEit.

6. MESVision failed to undertake adequate measures to ensure that MOVEit safeguarded the PII of Plaintiff and the proposed Class Members, including failing to ensure that MOVEit implemented industry standards for data security, and properly trained employees on cybersecurity protocols, resulting in the Data Breach.

7. Although MESVision discovered the Data Breach on or about August 23, 2023, Defendant failed to promptly notify and warn Data Breach victims of the unauthorized disclosure of their PII for three more months, preventing them from taking necessary steps to protect themselves from injury and harm.

8. As a direct and proximate result of Defendant's failures to protect Plaintiff's and the Class Members' sensitive PII and warn them promptly and fully about the Data Breach, Plaintiff and the proposed Class have suffered widespread injury and damages necessitating Plaintiff seeking relief on a class wide basis.

PARTIES

9. Plaintiff Eric E. Eufusia is a natural person and a citizen of the State of California, residing in Santa Rosa, California, where he intends to remain. Plaintiff Deutsch receives vision

[6] **Exhibit A.**

insurance benefits from MESVision and received a letter from MESVision notifying him that his PII was compromised in the Data Breach, and thus he is a Data Breach victim. [7]

10. Defendant, MESVision, is a California corporation, with its headquarters located at 20081 Ellipse, Foothill Ranch, California 92610.

11. MESVision's registered agent is located at 330 N. Brand Boulevard, Glendale, California.

JURISDICTION AND VENUE

12. The Court has personal jurisdiction over Defendant because MESVision resides in and does business in the State of California.

13. This is a class action brought pursuant to Cal. Civ. Proc. Code § 382, and this Court has jurisdiction over the Plaintiff's claims because the amount in controversy exceeds this Court's jurisdictional minimum.

14. Venue is proper under Cal. Civ. Proc. Code § 395(a) because Defendant resides in this County.

STATEMENT OF FACTS

Defendant MESVision

15. MESVision manages vision benefits on behalf of employers and insurers. MESVision "provides vision care plans directly to thousands of employer groups and millions of plan members nationwide for leading health care organizations, insurance carriers, and self-funded employer group[s]."[8] "As a Specialized Health Care Service Plan, [MESVision] offer[s] vision care services directly to members."[9]

---

[7] *See* **Exhibit B**, MESVision Letter, Re: Notice of Data Security Breach, November 14, 2023 ("Breach Letter").
[8] https://www.mesvision.com/aboutUs (last visited Dec. 17, 2023).
[9] *Id.*

16. As a condition of receiving insurance benefit services from MESVision, Defendant requires its customers to provide it with their private, sensitive, PII, including their including their names, email addresses, addresses, telephone numbers, Social Security numbers, dates of birth, which it stores in its information technology systems, and which it provides its third party vendors, including MOVEit.

17. In collecting and maintaining PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their PII.

18. MESVision acknowledges the importance of maintaining the security of its customers' PII it collects, stating to Data Breach victims that it "takes the responsibility to protect the information of vision plan participants very seriously."[10]

19. In fact, MESVision maintains a Privacy Policy (attached as **Exhibit C**) and HIPAA Compliance Notice (attached as **Exhibit D**) that are posted on its website. The Privacy Policy likewise states that "MESVision is committed to the security and privacy of [its] customers' data[,]" and that the Privacy Policy "serves as [MESVision's] agreement with its customers and other parties about [its] data handling practices." The Privacy Policy further states:

[10] Ex. A.

PROTECTING YOUR INFORMATION

We want the Users' Business Information to remain as secure as reasonably possible. We combine industry-standard technical safeguards with training for those employees who are permitted to access our customers' Business Information. When Users purchase a product or service online, we use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption to encrypt their information before it is sent to us in order to ensure the integrity and privacy of the information that the Users provide to us via the Internet.

Many of our web-based services are hosted on servers that are co-located at a third-party facility with whom we have a contract providing for security measures. For example, hosted services data is submitted via SSL and TLS encryption and stored on a server equipped with industry standard firewalls.

Hosted data may include personally identifiable information and other information that belongs to our customers' own customers, website visitors, or other users. We will not review, share, distribute, or reference any such customer data except as provided in the service, or as may be required by law. Individual records of customer data may be viewed or accessed by authorized MESVision employees, or independent contractors only for the purpose of resolving a problem, support and service for the plan, or suspected violation of the service or license agreement, or as may be required by law. MESVision policy requires that both employees and consultants execute a confidentiality agreement before working for and with MESVision. Those employees that violate our Privacy Policy are subject to disciplinary action, up to and including termination.

Despite these security measures, we do not represent or warrant that Business Information will be protected against loss, misuse, attacks, or alteration by third parties. Customers are responsible for maintaining the security and confidentiality of their usernames and passwords.

Ex. C, Privacy Policy.

20. The HIPAA Compliance Notice states that MESVision is "committed to working together with [its] business associates, trading partners, providers, and vendors toward continued compliance with the HIPAA Standards to protect individually identifiable health information and to improve the efficiency of electronic healthcare transactions." Ex. D, p. 1. The HIPAA Compliance Notice further acknowledges:

> You, as a patient, have the following rights with respect to your protected health information maintained by MESVision:
> . . .
> - **Right to Breach Notifications.** You have the right to or will receive notification of breaches of your unsecured PHI.

(Ex. D, p. 3)

21. Despite the foregoing, MESVision provided its customers' PII, including that of Plaintiff and the proposed Class, to its third-party vendor, which was then stored in its vendors' systems, without MESVision ensuring that the vendor adequately safeguarded MESVision's customers' PII.

22. Despite recognizing its duty to do so, on information and belief, MESVision did not ensure that its vendor implemented reasonably cybersecurity safeguards or policies to protect its consumers' PII or supervised its information technology or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, there were significant vulnerabilities in the systems used to systems for cybercriminals to exploit and gain access to consumers' PII, resulting in the Data Breach.

23. In addition, MESVision, by and through its agents and employees, represented to its customers, Plaintiff and the proposed Class Members, that Defendant would adequately protect their PII and not disclose said information other than as authorized, including as set forth in its Privacy Policy.

24. Plaintiff and the proposed Class Members, current and former customers of MESVision, would not have entrusted their PII to Defendant in the absence of its promises to safeguard that information, including as set forth in its Privacy Policy.

25. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the proposed Class Members' PII, Defendant assumed legal and equitable duties to Plaintiff, and the members of the Proposed Class, and knew or should have known that it was responsible for protecting his and their PII from unauthorized disclosure.

26. At all times Plaintiff and the members of the proposed Class, have taken reasonable steps to maintain the confidentiality of their PII; and, Plaintiff and the proposed Class Members,

as current and former customers of MESVision, relied on Defendant to keep their PII confidential and securely maintained.

A. The Data Breach

27. Plaintiff and the proposed Class Members are current and former vision insurance plan members of Defendant, MESVision.

28. As a condition of providing vision insurance benefit services, Defendant collected the PII of its customers, Plaintiff and the proposed Class Members, including but not limited to their names, dates of birth, Social Security numbers, addresses, subscriber/member ID numbers, Policy Numbers, Group Numbers, and Claim Numbers.

29. In collecting and maintaining PII, Defendant implicitly agrees that it will safeguard the data using reasonable means according to industry standards, its internal policies, as well as state and federal law. This duty extends to MESVision entrustment customers' PII to its third party vendors.

30. Defendant provided Plaintiff's and the Class Members' PII to its third-party vendor, MOVEit, who MESVision uses as a secure file-transfer tool.[11]

31. On or about May 28, 2023, the PII of Plaintiff and the proposed Class Members which was entrusted to MESVision was unauthorizedly disclosed to cybercriminals in the Data Breach, a Clop ransomware or external system breach attack impacting the MOVEit Transfer tool and the PII stored within.

32. According to MESVision, as stated in the Data Breach Notice:

> On August 23, 2023, MESVision discovered that an unauthorized individual had accessed information on its MOVEit server by exploiting a vulnerability in MOVEit's system. MESVision immediately took the server offline, launched an investigation into the incident, and engaged a cybersecurity firm. It was determined

[11] Data Breach Notice, Exhibit A.

that the unauthorized individual exfiltrated information from the server on May 28, 2023, and May 31, 2023.

33. Further according to MESVision, its investigation revealed evidence that the server which was exfiltrated by the unauthorized third party "contained information about individuals who are enrolled in MESVision benefit plans." MESVision indicated that "following a detailed analysis," it determined the information affected may have included: name, date of birth, address, Social Security Number, subscriber/member ID numbers, Policy Numbers, Group Numbers, and Claim Numbers.[12]

34. In reality, the Data Breach was executed by the notorious Clop ransomware gang, which claimed responsibility for the cyberattack, exploiting the MOVEit Transfer and MOVEit Cloud vulnerability for nefarious purposes and exfiltrating Plaintiff's and the proposed Class Members' PII. Clop is one of the most active ransomware actors, having breached over 2,000 organizations directly or indirectly in the MOVEit Transfer tool or cloud cyberattacks.[13]

35. MESVision, a sophisticated health/vision benefits provider, knew or should have known of the tactics that groups like Clop employ.

36. Beginning on or about November 14, 2023, MESVision began notifying its customers of the Data Breach by letter, the Data Breach Notice.[14]

37. Therein, MESVision vaguely described the Data Breach as quoted above, and went onto say that, "MESVision has rebuilt the MOVEit system in accordance with vendor requirements and with our gold standard build requirements. Before reactivating the system, we took a number

[12] *Id*.
[13] "Matthew J. Schwartz, Bankinfosecurity.com, "Data Breach Toll Tied to Clop Group's MOVEit Attack Surges," Sept. 25, 2023, avail. at https://www.bankinfosecurity.com/data-breach-toll-tied-to-clop-groups-moveit-attacks-surges-a-23153 (last acc. Dec. 12, 2023).
[14] Data Breach Notice, Exhibit A.

of technical measures to validate the security protections put in place."[15]

38. In its Data Breach Notice, MESVision recognized the significant harm caused by the Data Breach. MESVision advised the Data Breach victims as follows:

> It is always advisable to remain vigilant against attempts at identity theft or fraud, which includes carefully reviewing online and financial accounts, credit reports, and Explanations of Benefits ("EOBs") from your health insurers for suspicious activity. This is a best practice for all individuals. If you identify suspicious activity, you should contact the company that maintains the account, credit report, or EOB. Additional information about how to protect your identity is contained in Attachment B.

39. Furthermore, MESVision offered Data Breach victims one year of complimentary credit monitoring and identity restoration services through Kroll.[16] However, in order to take advantage of those services, the Data Breach victims must enroll by February 14, 2024.[17]

40. Despite its duties and alleged commitments to safeguard PII, Defendant did not in fact follow industry standard practices in securing consumers' PII and ensuring that its vendor properly secured customers' PII, as evidenced by the Data Breach.

41. MESVision failed to adequately protect the PII of its current and former customers, Plaintiff and the proposed Class Members, stored in its networks and which MESVision gave to MOVEit, resulting in the Data Breach.

42. MESVision failed to ensure that its vendor, MOVEit, employed adequate cybersecurity measures and adequately trained its employees on reasonable cybersecurity protocols to protect MESVision's customers' PII, causing the PII of Plaintiff and the proposed Class Members to be unauthorizedly disclosed in the Data Breach.

43. As a result of the Data Breach, its victims face a lifetime risk of identity theft, as it

---

[15] *Id.*
[16] *Id.*
[17] *Id.*

includes sensitive information that cannot be changed, like their dates of birth and Social Security numbers. Accordingly, any credit monitoring and identity theft protection which MESVision may offer is wholly insufficient to compensate Plaintiff and the Class Members for their damages resulting therefrom.

44. Indeed, as a result of the Data Breach which Defendant permitted to occur by virtue of its inadequate data security practices, Plaintiff and the proposed Class Members have suffered injury and damages, as set forth herein.

B. The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

45. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the file-transfer software industry preceding the date of the breach, including recent similar attacks against secure file transfer companies like Accellion and Fortra carried out by the same Russian cyber gang, Clop.[18]

46. In light of recent high profile data breaches at other file-transfer software companies, Defendant knew or should have known that its electronic records and consumers' PII would be targeted by cybercriminals.

47. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[19] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[20]

---

[18] *See* https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomwaregang/ (last visited on June 21, 2023); *see also* https://www.bleepingcomputer.com/news/security/fortra-sharesfindings-on-goanywhere-mft-zero-day-attacks/ (last visited on June 21, 2023).

[19] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 13, 2023).

[20] *Id*.

48. Indeed, cyberattacks have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [21]

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

C. Plaintiff Eric Eufusia's Experience

50. Plaintiff receives vision insurance benefits through MESVision.

51. Plaintiff was notified by MESVision of the Data Breach by letter, which he received in or around November 2023 ("Data Breach Notice, Ex. A").

52. Plaintiff entrusted his PII to MESVision as a condition of receiving vision plan services, including but not limited to his name, date of birth, address, and Social Security Number.

53. On information and belief, MESVision utilized MOVEit as a third-party vendor, and entrusted it with Plaintiff's and Class Members' valuable PII, which was stored in MOVEit's systems.

54. As a direct and proximate result of the Data Breach, Plaintiff has suffered, and imminently will suffer, injury-in-fact and damages, and his PII has been found on the Dark Web.

55. As a result of the Data Breach, Plaintiff experienced a fraudulent hotel charge in the amount of $690.00 on his Chase Business card following receipt of the Data Breach

[21] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited June 13, 2023).

Notice Letter.

56. As a result of the Data Breach, Plaintiff has and will spend time dealing with the consequences of the Data Breach, which will include time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. He has already spent two (2) hours reviewing accounts to mitigate the consequences of the date breach. This time has been lost forever and cannot be recaptured.

57. Plaintiff has experienced feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

58. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

59. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

60. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

D. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

61. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

62. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class Members have suffered and will continue to suffer damages, including unauthorized disclosure of this PII onto the Dark Web, monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

63. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

64. The value of Plaintiff's and the Class's PII on the black market is considerable.

Stolen PII trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

65. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

66. One such example of criminals using PII for profit is the development of "Fullz" packages.

67. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

68. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

69. Defendant disclosed the PII of Plaintiff and the Class to its vendor, MOVEit, who failed to take adequate measures to safeguard that PII, which was unauthorizedly

disclosed in the Data Breach for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

70. Defendant's failure to promptly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

E. Defendant failed to adhere to FTC guidelines.

71. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

72. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of Private Information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the

system; and have a response plan ready in the event of a breach.[22]

73. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[23]

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

75. These FTC enforcement actions include actions against entities failing to safeguard Private Information such as Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

76. MESVision failed to ensure that the vendor to whom Defendant gave its customers' PII properly implemented basic data security practices widely known throughout the industry.

77. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient Private Information constitutes an unfair act or practice

[22] *See* Federal Trade Commission, October 2016, "Protecting Private information: A Guide for Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last acc. Apr. 14, 2023).
[23] *See id*.

prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

78. Defendant was at all times fully aware of its obligations to protect the PII of its current and former customers. Defendant was also aware of the significant repercussions that would result from their failure to do so.

F. Defendant Fails to Comply with Industry Standards

79. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

80. Several best practices have been identified that a minimum should be implemented by employers in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

81. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

82. Defendant failed to ensure that its vendor, MOVEit, to whom it gave Plaintiff's and the proposed Class Members' PII, met the minimum standards of any of the following

frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

83. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to ensure that its vendor complied with at least one–or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

84. Plaintiff sues individually on behalf of himself, and on behalf of the proposed nationwide class ("Nationwide Class" or "Class"), defined as follows:

> **All individuals who were customers of Defendant and/or who entrusted their PII to Defendant and whose PII was compromised in the Data Breach and MOVEit vulnerability.**

85. Additionally, Plaintiff seeks to represent the following California Subclass, defined as:

> **All California citizens who were customers of Defendant and/or who entrusted their PII to Defendant and whose PII was compromised in the Data Breach and MOVEit vulnerability.**

86. Excluded from the Class is Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

87. Plaintiff reserves the right to amend the class definition.

88. **Numerosity**. Plaintiff is representative of the Class, consisting of, upon information and belief, more than 350,000, members, far too many to join in a single action;

89. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control.

90. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

91. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. His interests do not conflict with the Class's interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

92. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII, including exercising reasonable care in ensuring that its vendors to whom it gave PII adequately safeguarded customers' PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach and failed to ensure that its vendors implemented and maintained reasonable

security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant were negligent in maintaining, protecting, and securing PII including whether Defendant was negligent in ensuring that its vendors maintained, protected, and secured PII;

iv. Whether Defendant breached contractual promises to safeguard Plaintiff's and the Class's PII;

v. Whether Defendant violated the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150, *et seq*.;

vi. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vii. Whether Defendant's Data Breach Notice was reasonable;

viii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

ix. What the proper damages measure is; and

x. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

93. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

94. Plaintiff realleges all paragraphs as if fully set forth below.

95. Plaintiff and members of the Class entrusted their PII to Defendant, and Defendant gave that PII to a third party vendor. Defendant owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access, and ensuring that its vendor implemented industry-standard security procedures sufficient to reasonably protect the PII from the Data Breach, theft, and unauthorized use that came to pass, promptly detected attempts at unauthorized access.

96. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security, and failing to ensure that its vendor adequately safeguarded their PII in accordance with state-of-the-art industry standards concerning data security, would result in the compromise of that PII —just like the Data Breach that ultimately came to pass.

97. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's PII by disclosing and providing access to this information to third parties that did not adequately protect this PII and to unauthorized third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

98. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature,

and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

99. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and the Class's PII.

100. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII —whether by malware or otherwise.

101. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

102. Defendant breached its duties by failing to exercise reasonable care in supervising its employees, agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury.

103. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact.

104. As a direct and traceable result of Defendant's negligence and/or negligent

supervision, Plaintiff and the Class have suffered or will suffer injury and damages as set forth in the preceding paragraphs, including unauthorized disclosure of PII onto the Dark Web, monetary losses, lost time, anxiety, and emotional distress; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of stolen PII; and the continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

105. As a result, Plaintiff and the Class Members are entitled to recover actual and compensatory damages in an amount to be proven at trial, and punitive damages.

106. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) properly notify affected victims of the Data Breach, including identifying its vendor (ii) strengthen their data security systems and monitoring procedures, including with respect to its vendor's data security systems; and (iii) submit to future annual audits of those systems and monitoring procedures.

107. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class Members have no

adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

108. Plaintiff realleges all paragraphs as if fully set forth below.

109. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's PII and/or to ensure that its vendor provided fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

110. Section 5 of the FTC Act prohibits "unfair…practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, consumers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's PII.

111. Defendant breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII and/or failing to ensure that its vendor provided fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

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

113. Defendant violated its duty under Section 5 of the FTC Act by failing to use, or

failing to ensure that its vendor used, reasonable measures to protect Plaintiff's and the Class's PII and by not complying with, or failing to ensure that its vendor complied with, applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant collected and stored and the foreseeable consequences of a data breach and which it have to its vendors, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass in the Data Breach.

114. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

115. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

116. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

117. Had Plaintiff and the Class Members known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

118. Defendant's various violations and its failure to comply with applicable laws

and regulations constitutes negligence *per se*.

119. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, injury and damages, including unauthorized disclosure of PII onto the Dark Web, monetary losses, lost time, anxiety, and emotional distress; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of stolen PII; and the continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession, entitling them to actual and compensatory damages in an amount to be proven at trial, as well as punitive damages.

COUNT III
BREACH OF CONTRACT
(On Behalf of Plaintiff and the Class)

120. Plaintiff realleges all paragraphs as if fully set forth below.

121. Defendant offered to provide vision insurance benefit services to Plaintiff and Class Members in exchange for payment, a portion of which was paid for adequate data security.

122. Defendant also required Plaintiff and the Class Members to provide MESVision with their PII to receive financial services.

123. In turn, Defendant impliedly promised to protect Plaintiff's and the Class Members'

PII through adequate data security measures and to ensure that its vendors to whom MESVision gave customers' PII utilized adequate data security measures, as manifested by Defendant's conduct, and representations, including those found in MESVision's Privacy Policy related to "safeguarding [its] customers' data[.]"[24]

124. Plaintiff and the members of the Class accepted Defendant's offer by providing PII to MESVision in exchange for receiving Defendant's vision insurance benefit services, and then by paying for and receiving the same.

125. The valid and enforceable implied contracts that Plaintiff and Class Members entered into with Defendant included Defendant's promise to protect nonpublic Private Information given to Defendant from unauthorized disclosures. Plaintiff and Class Members provided their PII to MESVision in reliance of that promise.

126. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's and its vendor's data security practices complied with industry standards and relevant laws and regulations, including the FTC Act.

127. Plaintiff and Class Members reasonably believed and expected that Defendant would adequately employ adequate data security to protect that PII, and endure that MESVision's vendors to whom Defendant gave Plaintiff's and the Class Members' PII employed adequate data security to protect that PII. Defendant failed to do so.

128. Under the implied contracts, Defendant promised and was obligated to: (a) provide vision insurance benefit services to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' PII and/or ensure that its vendors protected Plaintiff's and the Class Members' PII: (i) provided to obtain such services and/or (ii) created in connection

[24] Exhibit C, Privacy Policy.

therewith. In exchange, Plaintiff and Class Members agreed to pay money for these services and to turn over their PII to Defendant.

129. Both the provision of these insurance benefit services, and the protection of Plaintiff's and Class Members' Private Information, including through MESVision's vendors, were material aspects of these implied contracts.

130. Plaintiff and Class Members would not have entrusted their PII to Defendant and entered into these implied contracts with Defendant without an understanding that their PII would be safeguarded and protected, or entrusted their PII to Defendant, in the absence of their implied promise to monitor their or their vendor's computer systems and networks to ensure that PII was not disclosed to unauthorized parties and exposed to the public as occurred in the Data Breach.

131. A meeting of the minds occurred when Plaintiff and the Class Members agreed to, and did, provide their PII to Defendant and paid for services for, amongst other things, (a) the provision of such services and (b) the protection of their PII.

132. Plaintiff and the Class Members performed their obligations under the contracts when they paid for services, and provided their PII, and payment, to Defendant.

133. Defendant materially breached its contractual obligations to protect the nonpublic PII of Plaintiff and the Class Members and to ensure that its vendors protected their nonpublic PII, which Defendant required and gathered, and then gave to its vendor, when the information was unauthorized disclosed in the Data Breach.

134. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to

their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

135. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

136. Defendant's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

137. The Data Breach was a reasonably foreseeable consequence of Defendant's conduct, by acts of omission or commission, in breach of these contracts, including failing to supervise its vendors to whom MESVision gave its customers' PII.

138. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, including failing to supervise its vendors for the protection of PII, Plaintiff and Class Members did not receive the full benefit of their bargains, and instead received services that were of a diminished value compared to those described in the contracts. Plaintiff and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

139. The injury, losses and damages Plaintiff and Class Members sustained that are described herein were the direct and proximate result of Defendant's breach of the implied contracts with them, including breach of the implied covenant of good faith and fair dealing.

140. Plaintiff and the Class Members are entitled to actual, compensatory and consequential, and nominal damages suffered as a result of the Data Breach.

141. Plaintiff and Class Members are also entitled to injunctive relief requiring

Defendant to (i) properly notify affected victims of the Data Breach, including identifying its vendor (ii) strengthen their data security systems and monitoring procedures, including with respect to its vendor's data security systems; and (iii) submit to future annual audits of those systems and monitoring procedures.

142. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class Members.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

143. Plaintiff realleges all paragraphs as if fully set forth below.

144. Plaintiff and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII to provide vision insurance benefit services, and then MESVision gave that PII to its vendors.

145. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members. And Defendant benefited from receiving Plaintiff's and Class members' PII, as this was used to provide file financial services.

146. Plaintiff and Class members reasonably understood that Defendant would use, and require its vendors to whom PII was given to use, adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

147. Defendant enriched itself by saving the costs it reasonably should have

expended on data security measures to secure Plaintiff's and Class members' PII, or saving the costs it reasonably should have expended to ensure that its vendors employed data security measures to secure this PII.

148. Instead of providing, or ensuring that its vendors provided, a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures and/or vendors who employed cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security and ensure that its vendors did so.

149. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' payment because Defendant failed to adequately protect their PII.

150. Plaintiff and Class members have no adequate remedy at law.

151. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT V
INVASION OF PRIVACY—INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Class)

152. Plaintiff realleges all paragraphs as if fully set forth below.

153. Plaintiff and the Class Members had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

154. Defendant owed a duty to Plaintiff and the Class Members to keep their PII confidential and to ensure that its vendors to whom MESVision disclosed Plaintiffs' and Class Members' PII kept that PII confidential.

155. Defendant failed to protect said PII and failed to ensure that its vendors protected said PII and exposed the PII of Plaintiff and the Class Members to unauthorized persons in the Data Breach.

156. Defendant allowed unauthorized third parties access to and examination of the PII of Plaintiff and the Class Members, by way of Defendant's failure to protect the PII and ensure that its vendors protected that PII.

157. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Class Members is highly offensive to a reasonable person.

158. The intrusion was into a place which a reasonable person would consider private and which is entitled to be private. Plaintiff's and the Class Members' PII was disclosed to Defendant in connection with receiving vision insurance benefit services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

159. The Data Breach constitutes an intentional or reckless interference by Defendant with Plaintiff's and the Class Members' privacy, of a kind that would be highly offensive to a reasonable person.

160. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because they had actual knowledge that its data security practices, including the supervision of its vendors' data security practices, were inadequate and insufficient.

161. Defendant acted with reckless disregard for Plaintiff's and Class Members' privacy when it allowed improper access to its systems containing Plaintiff's and Class Members' PII, or when it transmitted Plaintiff's and Class Members' PII to its vendor without ensuring the vendor utilized adequate data security measures to protect that PII.

162. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and implement appropriate policies to prevent the unauthorized release of Plaintiff's and Class Members' PII, and/or failed to ensure that its vendor adequately safeguarded its systems and implemented appropriate policies to prevent the unauthorized release of Plaintiff's and Class Members' PII.

163. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class Members.

164. As a direct and proximate result of the Defendant's invasion of privacy—intrusion into seclusion, Plaintiff and Class Members have suffered injury and damages as set forth herein, including but not limited to unauthorized disclosure of PII onto the Dark Web, monetary losses, lost time, anxiety, and emotional distress; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of stolen PII; and the continued risk to their PII, which

remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession

165. Plaintiff and the Class Members are entitled to compensatory, actual, and punitive damages as a result of Defendant's invasion of privacy in the Data Breach.

COUNT VI
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

166. Plaintiff realleges all paragraphs as if fully set forth below.

167. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

168. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of MESVision's relationship with its customers, in particular, to keep secure their PII.

169. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' PII and/or by failing to ensure that its vendors to whom Defendant transmitted Plaintiffs' and the Class Members' PII encrypted and otherwise protected the integrity of the systems containing Plaintiff's and Class Members' PII.

170. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

171. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII.

172. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury and damages, including but not limited to: unauthorized disclosure of PII onto the Dark Web, monetary losses, lost time, anxiety, and emotional distress; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of stolen PII; and the continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

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

174. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and the Class Members are entitled to compensatory, actual, and punitive damages as a result of the Data Breach.

COUNT VII
Violation of the California Consumer Privacy Act
Cal. Civ. Code § 1798.150
(On Behalf of Plaintiff and the California Subclass)

175. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

176. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Personal Information of Plaintiff and the California Subclass. As a direct and proximate result, Plaintiff's, and the California Subclass's nonencrypted and nonredacted Personal Information was subject to unauthorized access and exfiltration, theft, or disclosure.

177. Defendant is a business organized for the profit and financial benefit of its owners according to California Civil Code § 1798.140, that collects the personal information of its customers and employees, and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

178. Plaintiff and California Subclass Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards Personal Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold PII, including Plaintiff's and California Subclass members' Personal Information. Plaintiff and California Subclass members have an interest in ensuring that their Personal Information is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

179. Pursuant to California Civil Code § 1798.150(b), on December 20, 2023, Plaintiff mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific

provisions of the CCPA that Defendant has violated and continues to violate.

180. Accordingly, because no cure is possible under these facts and circumstances—Plaintiff intends to seek statutory damages of between $100 and $750, in addition to all other relief afforded by the CCPA.

PRAYER FOR RELIEF

Plaintiff, Eric E. Eufusia, demands a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, and punitive damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the

evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

Dated: December 21, 2023

Respectfully submitted,

/s/ Natalie A. Lyons
Natalie A. Lyons (293026)
Vess A. Miller (278020)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
nlyons@cohenandmalad.com
vmiller@cohenandmalad.com

Lynn A. Toops (*Pro Hac Vice* forthcoming
Amina A. Thomas (*Pro Hac Vice* forthcoming)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina Borelli (*Pro Hac Vice* forthcoming)
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
(608) 237-1775
(608) 509-4423 (facsimile)

sam@turkestrauss.com
raina@turkestrauss.com

Counsel for Plaintiff and the Proposed Class