

1 Scott Edward Cole, Esq. (S.B. #160744)
2 Laura Grace Van Note, Esq. (S.B. #310160)
3 **COLE & VAN NOTE**
4 555 12th Street, Suite 2100
5 Oakland, California 94607
6 Telephone: (510) 891-9800
7 Facsimile: (510) 891-7030
8 Email: sec@colevannote.com
9 Email: lvn@colevannote.com

10 Attorneys for Representative Plaintiff
11 and the Plaintiff Class

12
13 **UNITED STATES DISTRICT COURT**
14 **SOUTHERN DISTRICT OF CALIFORNIA**

15 MICHAEL SHUTA, individually,
16 and on behalf of all others similarly
17 situated,

18 Plaintiff,

19 v.

20 ALTMAN SPECIALTY PLANTS,
21 LLC,

22 Defendant.

Case No. '24CV1686 H BLM

CLASS ACTION

COMPLAINT

[JURY TRIAL DEMANDED]

23 **INTRODUCTION**

24 1. Representative Plaintiff Michael Shuta (“Representative Plaintiff”)
25 brings this class action against Defendant Altman Specialty Plants, LLC
26 (“Defendant”) for its failure to properly secure and safeguard Representative
27 Plaintiff’s and/or Class Members’ protected health information and personally
28 identifiable information stored within Defendant’s information network, including,
without limitation, names, Social Security numbers, dates of birth, financial and
payment card information, driver’s license and passport numbers, employer

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 identification numbers, health insurance data, medical information and usernames
2 with passwords (these types of information, *inter alia*, being thereafter referred to,
3 collectively, as “personally identifiable information” or “PII”).¹ All such
4 information is referred to in the aggregate herein as “Private Information.”

5 2. With this action, Representative Plaintiff seeks to hold Defendant
6 responsible for the harms it caused and will continue to cause Representative
7 Plaintiff and other similarly situated persons in the massive and preventable
8 cyberattack purportedly discovered by Defendant on September 11, 2023, by which
9 cybercriminals infiltrated Defendant’s inadequately protected network and accessed
10 the Private Information which was being kept under-protected (the “Data Breach”).

11 3. While Defendant claims to have discovered the breach as early as
12 September 11, 2023, Defendant did not begin informing victims of the Data Breach
13 until September 12, 2024, and failed to inform victims when or for how long the
14 Data Breach occurred. Indeed, Representative Plaintiff and Class Members were
15 wholly unaware of the Data Breach until they received letters from Defendant
16 informing them of it. The Notice received by Representative Plaintiff was dated
17 September 12, 2024.

18 4. Defendant acquired, collected and stored Representative Plaintiff’s and
19 Class Members’ Private Information. Therefore, at all relevant times, Defendant
20 knew or should have known that Representative Plaintiff and Class Members would
21 use Defendant’s services to store and/or share sensitive data, including highly
22 confidential Private Information.

23
24
25 ¹ Personally identifiable information (“PII”) generally incorporates information
26 that can be used to distinguish or trace an individual’s identity, either alone or
27 when combined with other personal or identifying information. 2 C.F.R. § 200.79.
28 At a minimum, it includes all information that on its face expressly identifies an
individual. PII also is generally defined to include certain identifiers that do not on
its face name an individual, but that are considered to be particularly sensitive
and/or valuable if in the wrong hands (for example, Social Security numbers,
passport numbers, driver’s license numbers, financial account numbers, etc.).

1 5. Defendant disregarded the rights of Representative Plaintiff and Class
 2 Members by intentionally, willfully, recklessly and/or negligently failing to take and
 3 implement adequate and reasonable measures to ensure that Representative
 4 Plaintiff’s and Class Members’ Private Information was safeguarded, failing to take
 5 available steps to prevent an unauthorized disclosure of data, and failing to follow
 6 applicable, required and appropriate protocols, policies and procedures regarding the
 7 encryption of data, even for internal use. As a result, Representative Plaintiff’s and
 8 Class Members’ Private Information was compromised through disclosure to an
 9 unknown and unauthorized third party—an undoubtedly nefarious third party
 10 seeking to profit off this disclosure by defrauding Representative Plaintiff and Class
 11 Members in the future. Representative Plaintiff and Class Members have a
 12 continuing interest in ensuring their information is and remains safe and are entitled
 13 to injunctive and other equitable relief.

14 **JURISDICTION AND VENUE**

15
 16 6. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity
 17 jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction
 18 over this action under 28 U.S.C. § 1332(d) because this is a class action where the
 19 amount in controversy exceeds the sum or value of \$5 million, exclusive of interest
 20 and costs, there are more than 100 members in the proposed class and at least one
 21 other Class Member is a citizen of a state different from Defendant.

22 7. Supplemental jurisdiction to adjudicate issues pertaining to state law is
 23 proper in this Court under 28 U.S.C. § 1367.

24 8. Defendant is headquartered and routinely conducts business in the State
 25 where this District is located, has sufficient minimum contacts in this State and has
 26 intentionally availed itself of this jurisdiction by marketing and selling products and
 27 services, and by accepting and processing payments for those products and services
 28 within this State.

COLE & VAN NOTE
 ATTORNEYS AT LAW
 555 12TH STREET, SUITE 2100
 OAKLAND, CA 94607
 TEL: (510) 891-9800

1 9. Venue is proper in this Court under 28 U.S.C. § 1391 because a
2 substantial part of the events that gave rise to Representative Plaintiff’s claims took
3 place within this District, and Defendant does business in this Judicial District.

4 **PLAINTIFF**

5 10. Representative Plaintiff is an adult individual and, at all relevant times
6 herein, was a resident and citizen of the State of Alabama. Representative Plaintiff
7 is a victim of the Data Breach.

8 11. Defendant received highly sensitive Private Information from
9 Representative Plaintiff in connection with the services Plaintiff obtained. As a
10 result, Representative Plaintiff’s information was among the data accessed by an
11 unauthorized third party in the Data Breach.

12 12. At all times herein relevant, Representative Plaintiff is and was a
13 member of the Class.

14 13. Representative Plaintiff’s Private Information was exposed in the Data
15 Breach because Defendant stored and/or shared Representative Plaintiff’s Private
16 Information. Representative Plaintiff’s Private Information was within the
17 possession and control of Defendant at the time of the Data Breach.

18 14. Representative Plaintiff received a letter from Defendant stating
19 Representative Plaintiff’s Private Information was involved in the Data Breach (the
20 “Notice”).

21 15. As a result, Representative Plaintiff spent time dealing with the
22 consequences of the Data Breach, which included and continues to include, time
23 spent verifying the legitimacy and impact of the Data Breach, exploring credit
24 monitoring and identity theft insurance options, self-monitoring Representative
25 Plaintiff’s accounts and seeking legal counsel regarding Representative Plaintiff’s
26 options for remedying and/or mitigating the effects of the Data Breach. This time
27 has been lost forever and cannot be recaptured.
28

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 16. Representative Plaintiff suffered actual injury in the form of damages
2 to and diminution in the value of Representative Plaintiff's Private Information—a
3 form of intangible property that Representative Plaintiff entrusted to Defendant,
4 which was compromised in and as a result of the Data Breach.

5 17. Representative Plaintiff suffered lost time, annoyance, interference and
6 inconvenience as a result of the Data Breach and has anxiety and increased concerns
7 for the loss of privacy, as well as anxiety over the impact of cybercriminals
8 accessing, using and selling Representative Plaintiff's Private Information.

9 18. Representative Plaintiff suffered imminent and impending injury
10 arising from the substantially increased risk of fraud, identity theft and misuse
11 resulting from Representative Plaintiff's Private Information being placed in the
12 hands of unauthorized third parties/criminals.

13 19. Representative Plaintiff has a continuing interest in ensuring that
14 Representative Plaintiff's Private Information, which, upon information and belief,
15 remains backed up in Defendant's possession, is protected and safeguarded from
16 future breaches.

17
18 **DEFENDANT**

19 20. Defendant is a for-profit corporation with a principal place of business
20 located in Vista, CA. Defendant is the largest horticultural grower in the United
21 States and is a family-owned wholesale plant nursery.²

22 21. The true names and capacities of persons or entities, whether
23 individual, corporate, associate or otherwise, who may be responsible for some of
24 the claims alleged here are currently unknown to Representative Plaintiff.
25 Representative Plaintiff will seek leave of court to amend this Complaint to reflect
26 the true names and capacities of such responsible parties when their identities
27 become known.

28

² <https://altmanplants.com/who-we-are/> (last accessed Sept. 20, 2024).

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CLASS ACTION ALLEGATIONS

22. Representative Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of Representative Plaintiff and the following class (collectively, the “Class”):

Plaintiff Class:

“All individuals within the United States of America whose Private Information was exposed to unauthorized third parties as a result of the data breach allegedly discovered by Defendant on or before September 11, 2023.”

23. Excluded from the Class is the following individuals and/or entities: Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including, but not limited to, its departments, agencies, divisions, bureaus, boards, sections, groups, counsel and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

24. In the alternative, Representative Plaintiff may request additional subclasses as necessary based, e.g., on the types of Private Information that were compromised.

25. Representative Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and its motion for class certification.

26. This action has been brought and may properly be maintained as a class action under Federal Rules of Civil Procedure Rule 23 because there is a well-

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 defined community of interest in the litigation and membership in the proposed
2 Classes is easily ascertainable.

3 a. Numerosity: A class action is the only available method for the
4 fair and efficient adjudication of this controversy. The members
5 of the Plaintiff Classes are so numerous that joinder of all
6 members is impractical, if not impossible. Membership in the
7 Class will be determined by analysis of Defendant’s records.

8 b. Commonality: Representative Plaintiff and Class Members share
9 a community of interest in that there are numerous common
10 questions and issues of fact and law which predominate over any
11 questions and issues solely affecting individual members,
12 including, but not necessarily limited to:

- 13 1) Whether Defendant had a legal duty to Representative
14 Plaintiff and the Classes to exercise due care in collecting,
15 storing, using and/or safeguarding their Private Information;
- 16 2) Whether Defendant knew or should have known of the
17 susceptibility of its data security systems to a data breach;
- 18 3) Whether Defendant’s security procedures and practices to
19 protect its systems were reasonable in light of the measures
20 recommended by data security experts;
- 21 4) Whether Defendant’s failure to implement adequate data
22 security measures allowed the Data Breach to occur;
- 23 5) Whether Defendant failed to comply with its own policies
24 and applicable laws, regulations and industry standards
25 relating to data security;
- 26 6) Whether Defendant adequately, promptly and accurately
27 informed Representative Plaintiff and Class Members that
28 their Private Information had been compromised;
- 7) How and when Defendant actually learned of the Data Breach;
- 8) Whether Defendant’s conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of Representative Plaintiff’s and Class Members’ Private Information;
- 9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- 10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Representative Plaintiff’s and Class Members’ Private Information;
- 11) Whether Representative Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct; and

12) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Representative Plaintiff's claims are typical of the claims of the Plaintiff Class. Representative Plaintiff and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Representative Plaintiff in this class action is an adequate representative of each of the Plaintiff Classes in that the Representative Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Classes in their entirety. Representative Plaintiff anticipates no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Classes to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Classes, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

27. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to bring all Class Members before the Court.

28. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 appropriate with respect to the Classes in their entirety. Defendant’s policies and
2 practices challenged herein apply to and affect Class Members uniformly and
3 Representative Plaintiff’s challenge of these policies and practices hinges on
4 Defendant’s conduct with respect to the Classes in their entirety, not on facts or
5 law applicable only to Representative Plaintiff.

6 29. Unless a Class-wide injunction is issued, Defendant may continue in its
7 failure to properly secure the Private Information of Class Members, and Defendant
8 may continue to act unlawfully as set forth in this Complaint.

9 30. Further, Defendant has acted or refused to act on grounds generally
10 applicable to the Classes and, accordingly, final injunctive or corresponding
11 declaratory relief with regard to the Class Members as a whole is appropriate under
12 Rule 23(b)(2) of the Federal Rules of Civil Procedure.

13
14 **COMMON FACTUAL ALLEGATIONS**

15 **The Cyberattack**

16 31. In the course of the Data Breach, one or more unauthorized third parties
17 accessed Class Members’ Private Information. Representative Plaintiff was among
18 the individuals whose data was accessed in the Data Breach.

19 32. According to the Data Breach Notification and/or publicly filed
20 documents, Representative Plaintiff states, on information and belief, that
21 thousands/millions of persons were affected by the Data Breach.

22 33. Representative Plaintiff was provided the information detailed above
23 upon Representative Plaintiff’s receipt of a letter from Defendant. Representative
24 Plaintiff was not aware of the Data Breach until receiving that letter.

25 **Defendant’s Failed Response to the Breach**

26 34. Upon information and belief, the unauthorized third-party
27 cybercriminals gained access to Representative Plaintiff’s and Class Members’
28 Private Information with the intent of misusing the Private Information, including

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 marketing and selling Representative Plaintiff’s and Class Members’ Private
2 Information.

3 35. Not until long after it claims to have discovered the Data Breach did
4 Defendant begin sending the Notice to persons whose Private Information Defendant
5 confirmed was potentially compromised as a result of the Data Breach. The Notice
6 provided basic details of the Data Breach and Defendant’s recommended next steps.

7 36. Representative Plaintiff and Class Members were required to provide
8 their Private Information to Defendant in order to receive services. Thus, Defendant
9 created, collected and stored Representative Plaintiff’s and Class Members’ Private
10 Information with the reasonable expectation and mutual understanding that
11 Defendant would comply with its obligations to keep such information confidential
12 and secure from unauthorized access.

13 37. Despite this, Representative Plaintiff and the Class Members remain,
14 even today, in the dark regarding what particular data was stolen, the particular
15 malware used and what steps are being taken, if any, to secure their Private
16 Information going forward. Representative Plaintiff and Class Members are thus left
17 to speculate as to where their Private Information ended up, who has used it and for
18 what potentially nefarious purposes. Indeed, they are left to further speculate as to
19 the full impact of the Data Breach and how exactly Defendant intends to enhance its
20 information security systems and monitoring capabilities so as to prevent further
21 breaches.

22 38. Representative Plaintiff’s and Class Members’ Private Information
23 may end up for sale on the dark web, or simply fall into the hands of companies that
24 will use the detailed Private Information for targeted marketing without
25 Representative Plaintiff’s and/or Class Members’ approval. Either way,
26 unauthorized individuals can now easily access Representative Plaintiff’s and Class
27 Members’ Private Information.

28

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Defendant Collected/Stored Class Members’ Private Information

39. Defendant acquired, collected, stored and assured reasonable security over Representative Plaintiff’s and Class Members’ Private Information.

40. As a condition of its relationships with Representative Plaintiff and Class Members, Defendant required that Representative Plaintiff and Class Members entrust Defendant with highly sensitive and confidential Private Information. Defendant, in turn, stored that information on Defendant’s system that was ultimately affected by the Data Breach.

41. By obtaining, collecting and storing Representative Plaintiff’s and Class Members’ Private Information, Defendant assumed legal and equitable duties over the Private Information and knew or should have known that it was thereafter responsible for protecting Representative Plaintiff’s and Class Members’ Private Information from unauthorized disclosure.

42. Representative Plaintiff and Class Members have taken reasonable steps to maintain their Private Information’s confidentiality. Representative Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only and to make only authorized disclosures of this information.

43. Defendant could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Representative Plaintiff’s and Class Members’ Private Information.

44. Defendant’s negligence in safeguarding Representative Plaintiff’s and Class Members’ Private Information is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

1 45. Due to the high-profile nature of these breaches, and other breaches of
2 its kind, Defendant was and/or certainly should have been on notice and aware of
3 such attacks occurring in its industry and, therefore, should have assumed and
4 adequately performed the duty of preparing for such an imminent attack. This is
5 especially true given that Defendant is a large, sophisticated operation with the
6 resources to put adequate data security protocols in place.

7 46. And yet, despite the prevalence of public announcements of data breach
8 and data security compromises, Defendant failed to take appropriate steps to protect
9 Representative Plaintiff's and Class Members' Private Information from being
10 compromised.

11 **Defendant Had an Obligation to Protect the Stolen Information**

12 47. In failing to adequately secure Representative Plaintiff's and Class
13 Member's sensitive data, Defendant breached duties it owed Representative Plaintiff
14 and Class Members under statutory and common law.

15 48. Representative Plaintiff and Class Members surrendered their highly
16 sensitive Private Information to Defendant under the implied condition that
17 Defendant would keep it private and secure. Accordingly, Defendant also has an
18 implied duty to safeguard their Private Information, independent of any statute.

19 49. Defendant was also prohibited by the Federal Trade Commission Act
20 (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or
21 practices in or affecting commerce." The Federal Trade Commission (the "FTC")
22 has concluded that a company's failure to maintain reasonable and appropriate data
23 security for consumers' sensitive personal information is an "unfair practice" in
24 violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d
25 236 (3d Cir. 2015).

26 50. In addition to its obligations under federal and state laws, Defendant
27 owed a duty to Representative Plaintiff and Class Members to exercise reasonable
28 care in obtaining, retaining, securing, safeguarding, deleting and protecting the

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 Private Information in Defendant’s possession from being compromised, lost,
2 stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to
3 Representative Plaintiff and Class Members to provide reasonable security,
4 including consistency with industry standards and requirements, and to ensure that
5 its computer systems, networks and protocols adequately protected Representative
6 Plaintiff’s and Class Members’ Private Information.

7 51. Defendant owed a duty to Representative Plaintiff and Class Members
8 to design, maintain and test its computer systems, servers and networks to ensure
9 that all Private Information in its possession was adequately secured and protected.

10 52. Defendant owed a duty to Representative Plaintiff and Class Members
11 to create and implement reasonable data security practices and procedures to protect
12 all Private Information in its possession, including not sharing information with
13 other entities who maintained sub-standard data security systems.

14 53. Defendant owed a duty to Representative Plaintiff and Class Members
15 to implement processes that would immediately detect a breach of its data security
16 systems in a timely manner.

17 54. Defendant owed a duty to Representative Plaintiff and Class Members
18 to act upon data security warnings and alerts in a timely fashion.

19 55. Defendant owed a duty to Representative Plaintiff and Class Members
20 to disclose if its computer systems and data security practices were inadequate to
21 safeguard individuals’ Private Information from theft because such an inadequacy
22 would be a material fact in the decision to entrust their Private Information to
23 Defendant.

24 56. Defendant owed a duty of care to Representative Plaintiff and Class
25 Members because they were foreseeable and probable victims of any inadequate data
26 security practices.

27 57. Defendant owed a duty to Representative Plaintiff and Class Members
28 to encrypt and/or more reliably encrypt Representative Plaintiff’s and Class

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 Members’ Private Information and monitor user behavior and activity in order to
2 identity possible threats.

3

4 **Value of the Relevant Sensitive Information**

5 58. While the greater efficiency of electronic health records translates to
6 cost savings for providers, it also comes with the risk of privacy breaches. These
7 electronic health records contain a plethora of sensitive information (e.g., patient
8 data, patient diagnosis, lab results, medical prescriptions, treatment plans, etc.) that
9 is valuable to cybercriminals. One patient’s complete record can be sold for
10 hundreds of dollars on the dark web. As such, Private Information is a valuable
11 commodity for which a “cyber black market” exists in which criminals openly post
12 stolen payment card numbers, Social Security numbers and other personal
13 information on a number of underground internet websites.

14 59. The high value of Private Information to criminals is further evidenced
15 by the prices they will pay for it through the dark web. Numerous sources cite dark
16 web pricing for stolen identity credentials. For example, personal information can
17 be sold at a price ranging from \$40 to \$200, and bank details have a price range of
18 \$50 to \$200.³ Experian reports that a stolen credit or debit card number can sell for
19 \$5 to \$110 on the dark web.⁴ Criminals can also purchase access to entire company
20 data breaches from \$999 to \$4,995.⁵

21
22
23

24 ³ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital
Trends, Oct. 16, 2019, available at:

25 <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

26 ⁴ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*,
Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>.

28 ⁵ *In the Dark*, VPNOverview, 2019, available at:
<https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 60. Between 2005 and 2019, at least 249 million people were affected by
2 healthcare data breaches.⁶ Indeed, during 2019 alone, over 41 million healthcare
3 records were exposed, stolen, or unlawfully disclosed in 505 data breaches.⁷ In short,
4 these sorts of data breaches are increasingly common, especially among healthcare
5 systems, which account for 30.03 percent of overall health data breaches, according
6 to cybersecurity firm Tenable.⁸

7 61. These criminal activities have and will result in devastating financial
8 and personal losses to Representative Plaintiff and Class Members. For example, it
9 is believed that certain Private Information compromised in the 2017 Equifax data
10 breach was being used three years later by identity thieves to apply for COVID-19-
11 related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat
12 for Representative Plaintiff and Class Members for the rest of their lives. They will
13 need to remain constantly vigilant.

14 62. The FTC defines identity theft as “a fraud committed or attempted using
15 the identifying information of another person without authority.” The FTC describes
16 “identifying information” as “any name or number that may be used, alone or in
17 conjunction with any other information, to identify a specific person,” including,
18 among other things, “[n]ame, Social Security number, date of birth, official State or
19 government issued driver’s license or identification number, alien registration
20 number, government passport number, employer or taxpayer identification number.”

21 63. Identity thieves can use Private Information, such as that of
22 Representative Plaintiff and Class Members which Defendant failed to keep secure,
23 to perpetrate a variety of crimes that harm victims. For instance, identity thieves may
24 commit various types of government fraud such as immigration fraud, obtaining a
25 driver’s license or identification card in the victim’s name but with another’s picture,

26 _____
27 ⁶ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/>.

28 ⁷ <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/>.

⁸ <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches/>.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 using the victim’s information to obtain government benefits or filing a fraudulent
2 tax return using the victim’s information to obtain a fraudulent refund.

3 64. The ramifications of Defendant’s failure to keep secure Representative
4 Plaintiff’s and Class Members’ Private Information are long lasting and severe. Once
5 Private Information is stolen, particularly identification numbers, fraudulent use of
6 that information and damage to victims may continue for years. Indeed,
7 Representative Plaintiff’s and Class Members’ Private Information was taken by
8 hackers to engage in identity theft or to sell it to other criminals who will purchase
9 the Private Information for that purpose. The fraudulent activity resulting from the
10 Data Breach may not come to light for years.

11 65. There may be a time lag between when harm occurs versus when it is
12 discovered and also between when Private Information is stolen and when it is used.
13 According to the U.S. Government Accountability Office (“GAO”), which
14 conducted a study regarding data breaches:

15 [L]aw enforcement officials told us that in some cases, stolen data may
16 be held for up to a year or more before being used to commit identity
17 theft. Further, once stolen data have been sold or posted on the Web,
18 fraudulent use of that information may continue for years. As a result,
19 studies that attempt to measure the harm resulting from data breaches
cannot necessarily rule out all future harm.⁹

20 66. The harm to Representative Plaintiff and Class Members is especially
21 acute given the nature of the leaked data. Medical identity theft is one of the most
22 common, most expensive and most difficult-to-prevent forms of identity theft.
23 According to Kaiser Health News, “medical-related identity theft accounted for 43
24 percent of all identity thefts reported in the United States in 2013,” which is more

25
26
27
28 ⁹ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:
<http://www.gao.gov/new.items/d07737.pdf/>.

1 than identity thefts involving banking and finance, the government and the military,
2 or education.¹⁰

3 67. “Medical identity theft is a growing and dangerous crime that leaves its
4 victims with little to no recourse for recovery,” reported Pam Dixon, executive
5 director of World Privacy Forum. “Victims often experience financial repercussions
6 and worse yet, they frequently discover erroneous information has been added to
7 their personal medical files due to the thief’s activities.”¹¹

8 68. When cybercriminals access financial information, health insurance
9 information and other personally sensitive data—as they did here—there is no limit
10 to the amount of fraud to which Defendant may have exposed Representative
11 Plaintiff and Class Members.

12 69. A study by Experian found that the average total cost of medical
13 identity theft is “about \$20,000” per incident, and that a majority of victims of
14 medical identity theft were forced to pay out-of-pocket costs for healthcare they did
15 not receive in order to restore coverage.¹² Almost half of medical identity theft
16 victims lose their healthcare coverage as a result of the incident, while nearly one-
17 third saw their insurance premiums rise, and 40 percent were never able to resolve
18 their identity theft at all.¹³

19 70. And data breaches are preventable.¹⁴ As Lucy Thompson wrote in the
20 DATA BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data
21 breaches that occurred could have been prevented by proper planning and the correct

22
23 ¹⁰ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser
Health News, Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/>.

24 ¹¹ *Id.*

25 ¹² Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET
(Mar. 3, 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/>.

26 ¹³ *Id.*; see also Healthcare Data Breach: What to Know About them and What to
Do After One, EXPERIAN, <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>.

27 ¹⁴ Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are
28 Preventable,” *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson,
ed., 2012).

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 design and implementation of appropriate security solutions.”¹⁵ She added that
2 “[o]rganizations that collect, use, store, and share sensitive personal data must accept
3 responsibility for protecting the information and ensuring that it is not
4 compromised....”¹⁶

5 71. Most of the reported data breaches are a result of lax security and the
6 failure to create or enforce appropriate security policies, rules and procedures.
7 Appropriate information security controls, including encryption, must be
8 implemented and enforced in a rigorous and disciplined manner so that a *data breach*
9 *never occurs*.¹⁷

10 72. Here, Defendant knew of the importance of safeguarding Private
11 Information and of the foreseeable consequences that would occur if Representative
12 Plaintiff’s and Class Members’ Private Information was stolen, including the
13 significant costs that would be placed on Representative Plaintiff and Class
14 Members as a result of a breach of this magnitude. As detailed above, Defendant
15 knew or should have known that the development and use of such protocols were
16 necessary to fulfill its statutory and common law duties to Representative Plaintiff
17 and Class Members. Its failure to do so is therefore intentional, willful, reckless
18 and/or grossly negligent.

19 73. Defendant disregarded the rights of Representative Plaintiff and Class
20 Members by, *inter alia*, (i) intentionally, willfully, recklessly and/or negligently
21 failing to take adequate and reasonable measures to ensure that its network servers
22 were protected against unauthorized intrusions, (ii) failing to disclose that it did not
23 have adequately robust security protocols and training practices in place to
24 adequately safeguard Representative Plaintiff’s and Class Members’ Private
25 Information, (iii) failing to take standard and reasonably available steps to prevent
26 the Data Breach, (iv) concealing the existence and extent of the Data Breach for an

27
28 ¹⁵ *Id.* at 17.
¹⁶ *Id.* at 28.
¹⁷ *Id.*

1 unreasonable duration of time, and (v) failing to provide Representative Plaintiff and
2 Class Members prompt and accurate notice of the Data Breach.

3
4
5 **FIRST CLAIM FOR RELIEF**
6 **Negligence**
7 **(On behalf of the Nationwide Class)**

8 74. Each and every allegation of the preceding paragraphs is incorporated
9 in this Count with the same force and effect as though fully set forth herein.

10 75. At all times herein relevant, Defendant owed Representative Plaintiff
11 and Class Members a duty of care, *inter alia*, to act with reasonable care to secure
12 and safeguard their Private Information and to use commercially reasonable methods
13 to do so. Defendant took on this obligation upon accepting and storing
14 Representative Plaintiff’s and Class Members’ Private Information on its computer
15 systems.

16 76. Among these duties, Defendant was expected:

- 17 a. to exercise reasonable care in obtaining, retaining, securing,
18 safeguarding, deleting and protecting the Private Information in
19 its possession;
- 20 b. to protect Representative Plaintiff’s and Class Members’ Private
21 Information using reasonable and adequate security procedures
22 and systems that were/are compliant with industry-standard
23 practices;
- 24 c. to implement processes to quickly detect the Data Breach and to
25 timely act on warnings about data breaches; and
- 26 d. to promptly notify Representative Plaintiff and Class Members
27 of any data breach, security incident or intrusion that affected or
28 may have affected their Private Information.

77. Defendant knew that the Private Information was private and
confidential and should be protected as private and confidential and, thus, Defendant
owed a duty of care not to subject Representative Plaintiff and Class Members to an
unreasonable risk of harm because they were foreseeable and probable victims of
any inadequate security practices.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 78. Defendant knew or should have known of the risks inherent in
2 collecting and storing Private Information, the vulnerabilities of its data security
3 systems and the importance of adequate security. Defendant knew about numerous,
4 well-publicized data breaches.

5 79. Defendant knew or should have known that its data systems and
6 networks did not adequately safeguard Representative Plaintiff's and Class
7 Members' Private Information.

8 80. Only Defendant was in the position to ensure that its systems and
9 protocols were sufficient to protect the Private Information that Representative
10 Plaintiff and Class Members had entrusted to it.

11 81. Defendant breached its duties to Representative Plaintiff and Class
12 Members by failing to provide fair, reasonable or adequate computer systems and
13 data security practices to safeguard Representative Plaintiff's and Class Members'
14 Private Information.

15 82. Because Defendant knew that a breach of its systems could damage
16 thousands of individuals, including Representative Plaintiff and Class Members,
17 Defendant had a duty to adequately protect its data systems and the Private
18 Information contained thereon.

19 83. Representative Plaintiff's and Class Members' willingness to entrust
20 Defendant with its Private Information was predicated on the understanding that
21 Defendant would take adequate security precautions. Moreover, only Defendant had
22 the ability to protect its systems and the Private Information it stored on them from
23 attack. Thus, Defendant had a special relationship with Representative Plaintiff and
24 Class Members.

25 84. Defendant also had independent duties under state and federal laws that
26 required Defendant to reasonably safeguard Representative Plaintiff's and Class
27 Members' Private Information and promptly notify them about the Data Breach.
28

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 These “independent duties” are untethered to any contract between Defendant and
2 Representative Plaintiff and/or the remaining Class Members.

3 85. Defendant breached its general duty of care to Representative Plaintiff
4 and Class Members in, but not necessarily limited to, the following ways:

- 5 a. by failing to provide fair, reasonable or adequate computer
6 systems and data security practices to safeguard Representative
7 Plaintiff’s and Class Members’ Private Information;
8 b. by failing to timely and accurately disclose that Representative
9 Plaintiff’s and Class Members’ Private Information had been
10 improperly acquired or accessed;
11 c. by failing to adequately protect and safeguard the Private
12 Information by knowingly disregarding standard information
13 security principles, despite obvious risks, and by allowing
14 unmonitored and unrestricted access to unsecured Private
15 Information;
16 d. by failing to provide adequate supervision and oversight of the
17 Private Information with which it was and is entrusted, in spite
18 of the known risk and foreseeable likelihood of breach and
19 misuse, which permitted an unknown third party to gather
20 Representative Plaintiff’s and Class Members’ Private
21 Information, misuse the Private Information and intentionally
22 disclose it to others without consent;
23 e. by failing to adequately train its employees to not store Private
24 Information longer than absolutely necessary;
25 f. by failing to consistently enforce security policies aimed at
26 protecting Representative Plaintiff’s and the Class Members’
27 Private Information;
28 g. by failing to implement processes to quickly detect data
breaches, security incidents or intrusions; and
h. by failing to encrypt Representative Plaintiff’s and Class
Members’ Private Information and monitor user behavior and
activity in order to identify possible threats.

86. Defendant’s willful failure to abide by these duties was wrongful,
reckless and/or grossly negligent in light of the foreseeable risks and known threats.

87. As a proximate and foreseeable result of Defendant’s grossly negligent
conduct, Representative Plaintiff and Class Members have suffered damages and are
at imminent risk of additional harms and damages (as alleged above).

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 88. The law further imposes an affirmative duty on Defendant to timely
2 disclose the unauthorized access and theft of the Private Information to
3 Representative Plaintiff and Class Members so that they could and/or still can take
4 appropriate measures to mitigate damages, protect against adverse consequences and
5 thwart future misuse of their Private Information.

6 89. Defendant breached its duty to notify Representative Plaintiff and Class
7 Members of the unauthorized access by waiting excessively after learning of the
8 Data Breach to notify Representative Plaintiff and Class Members and then by
9 failing and continuing to fail to provide Representative Plaintiff and Class Members
10 sufficient information regarding the breach. To date, Defendant has not provided
11 sufficient information to Representative Plaintiff and Class Members regarding the
12 extent of the unauthorized access and continues to breach its disclosure obligations
13 to Representative Plaintiff and Class Members.

14 90. Further, through its failure to provide timely and clear notification of
15 the Data Breach to Representative Plaintiff and Class Members, Defendant
16 prevented Representative Plaintiff and Class Members from taking meaningful,
17 proactive steps to, *inter alia*, secure and/or access their Private Information.

18 91. There is a close causal connection between Defendant's failure to
19 implement security measures to protect Representative Plaintiff's and Class
20 Members' Private Information and the harm suffered, or risk of imminent harm
21 suffered, by Representative Plaintiff and Class Members. Representative Plaintiff's
22 and Class Members' Private Information was accessed as the proximate result of
23 Defendant's failure to exercise reasonable care in safeguarding such Private
24 Information by adopting, implementing and maintaining appropriate security
25 measures.

26 92. Defendant's wrongful actions, inactions and omissions constituted (and
27 continue to constitute) common law negligence.
28

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 93. The damages Representative Plaintiff and Class Members have
2 suffered (as alleged above) and will continue to suffer were and are the direct and
3 proximate result of Defendant’s grossly negligent conduct.

4 94. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits “unfair
5 [...] practices in or affecting commerce,” including, as interpreted and enforced by
6 the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use
7 reasonable measures to protect Private Information. The FTC publications and
8 orders described above also form part of the basis of Defendant’s duty in this regard.

9 95. Defendant violated 15 U.S.C. § 45 by failing to use reasonable
10 measures to protect Private Information and not complying with applicable industry
11 standards, as described in detail herein. Defendant’s conduct was particularly
12 unreasonable given the nature and amount of Private Information it obtained and
13 stored and the foreseeable consequences of the immense damages that would result
14 to Representative Plaintiff and Class Members.

15 96. As a direct and proximate result of Defendant’s negligence,
16 Representative Plaintiff and Class Members have suffered and will continue to suffer
17 injury, including, but not limited to, (i) actual identity theft, (ii) the loss of the
18 opportunity of how their Private Information is used, (iii) the compromise,
19 publication and/or theft of their Private Information, (iv) out-of-pocket expenses
20 associated with the prevention, detection and recovery from identity theft, tax fraud
21 and/or unauthorized use of their Private Information, (v) lost opportunity costs
22 associated with effort expended and the loss of productivity addressing and
23 attempting to mitigate the actual and future consequences of the Data Breach,
24 including, but not limited to, efforts spent researching how to prevent, detect, contest
25 and recover from embarrassment and identity theft, (vi) lost continuity in relation to
26 their personal records, (vii) the continued risk to their Private Information, which
27 may remain in Defendant’s possession and is subject to further unauthorized
28 disclosures so long as Defendant fails to undertake appropriate and adequate

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 measures to protect Representative Plaintiff’s and Class Members’ Private
2 Information in its continued possession, and (viii) future costs in terms of time, effort
3 and money that will be expended to prevent, detect, contest and repair the impact of
4 the Private Information compromised as a result of the Data Breach for the remainder
5 of the lives of Representative Plaintiff and Class Members.

6 97. As a direct and proximate result of Defendant’s negligence,
7 Representative Plaintiff and Class Members have suffered and will continue to suffer
8 other forms of injury and/or harm, including, but not limited to, anxiety, emotional
9 distress, loss of privacy and other economic and noneconomic losses.

10 98. Additionally, as a direct and proximate result of Defendant’s
11 negligence, Representative Plaintiff and Class Members have suffered and will
12 continue to suffer the continued risks of exposure of their Private Information, which
13 remains in Defendant’s possession and is subject to further unauthorized disclosures
14 so long as Defendant fails to undertake appropriate and adequate measures to protect
15 Private Information in its continued possession.

16
17 **SECOND CLAIM FOR RELIEF**
18 **Breach of Implied Contract**
19 **(On behalf of the Nationwide Class)**

20 99. Each and every allegation of the preceding paragraphs is incorporated
21 in this Count with the same force and effect as though fully set forth herein.

22 100. Through their course of conduct, Defendant, Representative Plaintiff
23 and Class Members entered into implied contracts for Defendant to implement data
24 security adequate to safeguard and protect the privacy of Representative Plaintiff’s
25 and Class Members’ Private Information.

26 101. Defendant solicited, invited and required Representative Plaintiff and
27 Class Members to provide their Private Information as part of Defendant’s regular
28 business practices. Representative Plaintiff and Class Members accepted
Defendant’s offers by, in part, providing their Private Information to Defendant.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 102. As a condition of being direct customers and/or employees of
2 Defendant, Representative Plaintiff and Class Members provided and entrusted their
3 Private Information to Defendant. In so doing, Representative Plaintiff and Class
4 Members entered into implied contracts with Defendant by which Defendant agreed
5 to safeguard and protect such non-public information, to keep such information
6 secure and confidential and to timely and accurately notify Representative Plaintiff
7 and Class Members if its data had been breached and compromised or stolen.

8 103. A meeting of the minds occurred when Representative Plaintiff and
9 Class Members agreed to, and did, provide their Private Information to Defendant,
10 in exchange for, amongst other things, the protection of their Private Information.

11 104. Representative Plaintiff and Class Members fully performed their
12 obligations under the implied contracts with Defendant.

13 105. Defendant breached the implied contracts it made with Representative
14 Plaintiff and Class Members by failing to safeguard and protect their Private
15 Information and by failing to provide timely and accurate notice to them that their
16 Private Information was compromised as a result of the Data Breach.

17 106. As a direct and proximate result of Defendant’s above-described breach
18 of implied contract, Representative Plaintiff and Class Members have suffered and
19 will continue to suffer (i) ongoing, imminent and impending threat of identity theft
20 crimes, fraud and abuse, resulting in monetary loss and economic harm, (ii) actual
21 identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm,
22 (iii) loss of the confidentiality of the stolen confidential data, (iv) the illegal sale of
23 the compromised data on the dark web, (v) lost work time, and (f) other economic
24 and noneconomic harm.

25
26 **THIRD CLAIM FOR RELIEF**
27 **Breach of the Implied Covenant of Good Faith and Fair Dealing**
28 **(On behalf of the Nationwide Class)**

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 107. Each and every allegation of the preceding paragraphs is incorporated
2 in this Court with the same force and effect as though fully set forth therein.

3 108. Every contract in this State has an implied covenant of good faith and
4 fair dealing. This implied covenant is an independent duty and may be breached
5 even when there is no breach of a contract’s actual and/or express terms.

6 109. Representative Plaintiff and Class Members have complied with and
7 performed all conditions of their contracts with Defendant.

8 110. Defendant breached the implied covenant of good faith and fair
9 dealing by failing to maintain adequate computer systems and data security practices
10 to safeguard Private Information, failing to timely and accurately disclose the Data
11 Breach to Representative Plaintiff and Class Members and continued acceptance of
12 Private Information and storage of other personal information after Defendant knew
13 or should have known of the security vulnerabilities of the systems that were
14 exploited in the Data Breach.

15 111. Defendant acted in bad faith and/or with malicious motive in denying
16 Representative Plaintiff and Class Members the full benefit of their bargains as
17 originally intended by the parties, thereby causing them injury in an amount to be
18 determined at trial.

19
20 **FOURTH CAUSE OF ACTION**
21 **California Information Practices Act of 1977**
22 **Cal. Civ. Code § 1798, et seq.**

23 112. Each and every allegation of the preceding paragraphs is incorporated
24 in this cause of action with the same force and effect as though fully set forth herein.

25 113. Defendant was legally obligated to “establish appropriate and
26 reasonable administrative, technical and physical safeguards to ensure compliance
27 with the [Information Practices Act of 1977], to ensure the security and
28 confidentiality of records and to protect against anticipated threats or hazards to their
security or integrity which could result in any injury.” Cal. Civ. Code § 1798.21.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 114. Defendant failed to establish appropriate and reasonable administrative,
2 technical and physical safeguards to ensure compliance with the Information
3 Practices Act of 1977 with regard to the Private Information of Representative
4 Plaintiff and Class Members.

5 115. Defendant failed to ensure the security and confidentiality of records
6 containing the Private Information of Representative Plaintiff and Class Members.

7 116. Defendant failed to protect against anticipated threats and hazards to
8 the security and integrity of records containing the Private Information of
9 Representative Plaintiff and Class Members.

10 117. As a result of these failures, Representative Plaintiff and Class
11 Members have suffered and will continue to suffer economic damages and other
12 injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and
13 continuing increased risk of identity theft, identify fraud and medical fraud—risks
14 justifying expenditures for protective and remedial services for which they are
15 entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality
16 of their Private Information, (iv) deprivation of the value of their Private
17 Information, for which there is a well-established national and international market,
18 and/or (v) the financial and temporal cost of monitoring their credit, monitoring their
19 financial accounts and mitigating their damages.

20 118. Representative Plaintiff and Class Members are also entitled to
21 injunctive relief under California Civil Code § 1798.47.

22
23 **FIFTH CAUSE OF ACTION**
California Unfair Competition Law
24 **Cal. Bus. & Prof. Code §§ 17200, et seq.**

25 119. Each and every allegation of the preceding paragraphs is incorporated
26 in this cause of action with the same force and effect as though fully set forth herein

27 120. Defendant is a “person” as defined by Cal. Bus. & Prof. Code §17201.
28

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 121. Defendant violated Cal. Bus. & Prof. Code § 17200, *et seq.* (“UCL”)
2 by engaging in unlawful, unfair and deceptive business acts and practices.

3 122. Defendant’s “unfair” acts and practices include:

4 a. Defendant’s failure to implement and maintain reasonable
5 security measures to protect Representative Plaintiff’s and Class
6 Members’ Private Information from unauthorized disclosure,
7 release, data breaches and theft, which was a direct and
8 proximate cause of the Data Breach. Defendant failed to identify
9 foreseeable security risks, remediate identified security risks and
adequately maintain and/or improve security following previous
cybersecurity incidents. This conduct, with little if any utility, is
unfair when weighed against the harm to Representative Plaintiff
and Class Members, whose Private Information has been
compromised;

10 b. Defendant’s failure to implement and maintain reasonable
11 security measures, which was contrary to legislatively declared
12 public policy that seeks to protect consumers’ data and ensure
13 that entities that are trusted with it use appropriate security
14 measures. These policies are reflected in laws, including the FTC
15 Act (15 U.S.C. § 45, *et seq.*);

16 c. Defendant’s failure to implement and maintain reasonable
17 security measures, which also leads to substantial consumer
18 injuries, as described above, that are not outweighed by any
19 countervailing benefits to consumers or competition. Moreover,
20 because consumers could not know of Defendant’s inadequate
21 security, consumers could not have reasonably avoided the
22 harms that Defendant caused; and

23 d. Engaging in unlawful business practices by violating Cal. Civ.
24 Code § 1798.82.

25 123. Defendant has engaged in “unlawful” business practices by violating
26 multiple laws, including the FTC Act, 15 U.S.C. § 45, *et seq.*, and California
27 common law.

28 124. Defendant’s unlawful, unfair and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and
privacy measures to protect Representative Plaintiff’s and Class
Members’ Private Information, which was a direct and proximate
cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks,
remediate identified security and privacy risks and adequately
maintain and/or improve security and privacy measures, which
was a direct and proximate cause of the Data Breach;

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Representative Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Representative Plaintiff's and Class Members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Representative Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*;
- f. Omitting, suppressing and concealing the material fact that it did not reasonably or adequately secure Representative Plaintiff's and Class Members' Private Information; and
- g. Omitting, suppressing and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Representative Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*

125. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

126. As a direct and proximate result of Defendant's unfair, unlawful and fraudulent acts and practices, Representative Plaintiff and Class Members were injured and lost money or property, including the price received by Defendant for its goods and services, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft and loss of value of their Private Information.

127. Defendant acted intentionally, knowingly and maliciously to violate California's Unfair Competition Law and recklessly disregarded Representative Plaintiff's and Class Members' rights.

1 128. Representative Plaintiff and Class Members seek all monetary and
2 nonmonetary relief allowed by law, including restitution of all profits stemming
3 from Defendant’s unfair, unlawful and fraudulent business practices or use of their
4 Private Information, declaratory relief, reasonable attorneys’ fees and costs under
5 California Code of Civil Procedure § 1021.5, injunctive relief and other appropriate
6 equitable relief.

7
8 **RELIEF SOUGHT**

9 **WHEREFORE**, Representative Plaintiff, on Representative Plaintiff’s own
10 behalf and on behalf of each member of the proposed National Class and any
11 proposed subclass, respectfully requests that the Court enter judgment in favor of
12 Representative Plaintiff and the Class and for the following specific relief against
13 Defendant(s) as follows:

14 1. That the Court declare, adjudge and decree that this action is a proper
15 class action and certify each of the proposed Classes and/or any other appropriate
16 Subclasses under Federal Rules of Civil Procedure Rule 23 (b)(1), (b)(2), and/or
17 (b)(3), including appointment of Representative Plaintiff’s counsel as Class
18 Counsel;

19 2. For an award of damages, including actual, nominal and consequential
20 damages, as allowed by law in an amount to be determined;

21 3. That the Court enjoin Defendant, ordering it to cease and desist from
22 unlawful activities;

23 4. For equitable relief enjoining Defendant from engaging in the wrongful
24 conduct complained of herein pertaining to the misuse and/or disclosure of
25 Representative Plaintiff’s and Class Members’ Private Information, and from
26 refusing to issue prompt, complete and accurate disclosures to Representative
27 Plaintiff and Class Members;

28

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 5. For injunctive relief requested by Representative Plaintiff, including,
2 but not limited to, injunctive and other equitable relief as is necessary to protect the
3 interests of Representative Plaintiff and Class Members, including, but not limited
4 to, an Order:

- 5 a. prohibiting Defendant from engaging in the wrongful and
6 unlawful acts described herein;
- 7 b. requiring Defendant to protect, including through encryption, all
8 data collected through the course of business in accordance with
9 all applicable regulations, industry standards and federal, state or
10 local laws;
- 11 c. requiring Defendant to delete and purge Representative
12 Plaintiff's and Class Members' Private Information unless
13 Defendant can provide to the Court reasonable justification for
14 the retention and use of such information when weighed against
15 the privacy interests of Representative Plaintiff and Class
16 Members;
- 17 d. requiring Defendant to implement and maintain a comprehensive
18 Information Security Program designed to protect the
19 confidentiality and integrity of Representative Plaintiff's and
20 Class Members' Private Information;
- 21 e. requiring Defendant to engage independent third-party security
22 auditors and internal personnel to run automated security
23 monitoring, simulated attacks, penetration tests and audits on
24 Defendant's systems on a periodic basis;
- 25 f. prohibiting Defendant from maintaining Representative
26 Plaintiff's and Class Members' Private Information on a cloud-
27 based database;
- 28 g. requiring Defendant to segment data by creating firewalls and
access controls so that if one area of Defendant's network is
compromised, hackers cannot gain access to other portions of
Defendant's systems;
- h. requiring Defendant to conduct regular database scanning and
securing checks;
- i. requiring Defendant to establish an information security training
program that includes at least annual information security
training for all employees, with additional training to be provided
as appropriate based upon the employees' respective
responsibilities with handling Private Information, as well as
protecting the Private Information of Representative Plaintiff and
Class Members;
- j. requiring Defendant to implement a system of tests to assess its
respective employees' knowledge of the education programs

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested and updated; and

l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

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

8. For all other Orders, findings and determinations identified and sought in this Complaint.

JURY DEMAND

Representative Plaintiff, individually, and on behalf of the Plaintiff Class, hereby demands a trial by jury for all issues triable by jury.

Dated: September 20, 2024

By: /s/ Laura Grace Van Note
Laura Van Note, Esq. (CA S.B. #310160)
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: lvn@colevannote.com

Attorney for Representative Plaintiff and the Plaintiff Class

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Altman Specialty Plants September 2023 Data Breach Triggers Class Action Lawsuit](#)
