

1 John J. Nelson (SBN 317598)
2 **MILBERG COLEMAN BRYSON**
3 **PHILLIPS GROSSMAN, PLLC**
4 402 W. Broadway, Suite 1760
5 San Diego, CA 92101
6 Telephone: (858) 209-6941
7 Email: jnelson@milberg.com

8
9
10 **UNITED STATES DISTRICT COURT**
11 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**
12

13 KRISTIANNE SCOTT, on behalf of herself
14 individually and on behalf of all others
15 similarly situated,

16 Plaintiff,

17 v.

18 ADVANTIS GLOBAL, LLC,

19 Defendant.
20

21 Case No.: _____

22 **CLASS ACTION COMPLAINT**

23 **DEMAND FOR A JURY TRIAL**

24 Plaintiff Kristianne Scott (“Plaintiff”) brings this Class Action Complaint (“Complaint”) against Defendant Advantis Global, LLC (“Advantis” or “Defendant”) as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels’ investigation, and upon information and belief as to all other matters, as follows:

25 **INTRODUCTION**

26 1. This class action arises out of the recent cyberattack and data breach (“Data Breach”) that was perpetuated against Advantis, an IT staffing agency.

27 2. Plaintiff’s and Class Members’ sensitive personal information—which they entrusted to Defendant—was compromised and unlawfully accessed due to the Data Breach.
28

1 3. Advantis collected and maintained certain personally identifiable information of
2 Plaintiff and the putative Class Members (defined below), who are (or were) employees at
3 Advantis.

4 4. The PII compromised in the Data Breach included Plaintiff's and Class Members'
5 names and Social Security numbers, ("personally identifying information" or "PII").
6

7 5. The PII compromised in the Data Breach was targeted and exfiltrated by cyber-
8 criminals and remains in the hands of those cyber-criminals.

9 6. As a result of the Data Breach, Plaintiff and approximately 5,000 Class Members,¹
10 suffered concrete injury in fact including, but not limited to: (i) invasion of privacy; (ii) theft of
11 their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with
12 attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the
13 bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences
14 of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii)
15 statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to
16 their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and
17 abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized
18 disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect
19 the PII.
20
21
22
23
24

25
26 ¹ According to the breach report submitted to the Office of the Maine Attorney General, 5,666
27 persons were impacted in the Data Breach. See
28 <https://apps.web.maine.gov/online/aewiewer/ME/40/3904cf03-c64e-4719-b5cc-41e56363a10d.shtml>

1 7. The Data Breach was a direct result of Defendant’s failure to implement adequate
2 and reasonable cyber-security procedures and protocols necessary to protect its employees’ PII
3 from a foreseeable and preventable cyber-attack.

4 8. Plaintiff brings this class action lawsuit on behalf of those similarly situated to
5 address Defendant’s inadequate safeguarding of Class Members’ PII that it collected and
6 maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class
7 Members that their information had been subject to the unauthorized access by an unknown third
8 party and precisely what specific type of information was accessed.

9 9. Defendant maintained the PII in a reckless manner. In particular, the PII was
10 maintained on Defendant’s computer network in a condition vulnerable to cyberattacks. Upon
11 information and belief, the mechanism of the cyberattack and potential for improper disclosure of
12 Plaintiff’s and Class Members’ PII was a known risk to Defendant, and thus, Defendant was on
13 notice that failing to take steps necessary to secure the PII from those risks left that property in a
14 dangerous condition.

15 10. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*,
16 intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures
17 to ensure its data systems were protected against unauthorized intrusions; failing to disclose that
18 they did not have adequately robust computer systems and security practices to safeguard Class
19 Members’ PII; failing to take standard and reasonably available steps to prevent the Data Breach;
20 and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

21 11. Plaintiff’s and Class Members’ identities are now at risk because of Defendant’s
22 negligent conduct because the PII that Defendant collected and maintained is now in the hands of
23 data thieves.

1 mail, dated December 5, 2023 (the “Notice Letter”). If Ms. Scott had known that Defendant would
2 not adequately protect her PII, she would not have entrusted Defendant or anyone in Defendant’s
3 position with her PII or allowed Defendant to maintain this sensitive PII.

4 19. Defendant is limited liability company organized under the state laws of California
5 with its principal place of business located in Mill Valley, California.
6

7 **JURISDICTION AND VENUE**

8 20. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act
9 of 2005 (“CAFA”), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of
10 \$5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and
11 minimal diversity exists because many putative class members, including Plaintiff, are citizens of
12 a different state than Defendant. This Court also has supplemental jurisdiction pursuant to 28
13 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.
14

15 21. This Court has personal jurisdiction over Defendant because it operates and
16 maintains its principal place of business in this District and the computer systems implicated in
17 this Data Breach are likely based in this District. Further, Defendant is authorized to and regularly
18 conducts business in this District and makes decisions regarding corporate governance and
19 management of its businesses in this District, including decisions regarding the security measures
20 to protect its employees’ PII.
21

22 22. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because a
23 substantial part of the events giving rise to this action occurred in this District, including decisions
24 made by Defendant’s governance and management personnel or inaction by those individuals that
25 led to the Data Breach; Defendant’s principal place of business is located in this district; Defendant
26
27
28

1 maintains Class Members' PII in this District; and Defendant caused harm to Class Members
2 residing in this District.

3 **FACTUAL ALLEGATIONS**

4 ***Defendant's Business***

5 23. Defendant is an IT staffing agency.

6 24. Plaintiff and Class Members are current or former employees at Advantis.

7 25. As a condition of obtaining employment and/or obtaining certain employee benefits
8 at Defendant, Advantis requires that its employees, including Plaintiff and Class Members, entrust
9 it with highly sensitive personal information.
10

11 26. The information held by Defendant in its computer systems at the time of the Data
12 Breach included the unencrypted PII of Plaintiff and Class Members.

13 27. Upon information and belief, Defendant made promises and representations to its
14 employees, including Plaintiff and Class Members, that the PII collected from them as a condition
15 of their employment and/or receiving benefits at Defendant would be kept safe, confidential, that
16 the privacy of that information would be maintained, and that Defendant would delete any sensitive
17 information after it was no longer required to maintain it.
18

19 28. Indeed, Defendant provides on its website that: "[w]e strive to protect the security
20 of your personal data by use of appropriate measures and processes."²
21

22 29. Plaintiff and Class Members provided their PII to Defendant with the reasonable
23 expectation and on the mutual understanding that Defendant would comply with its obligations to
24 keep such information confidential and secure from unauthorized access.
25

26
27 _____
28 ² <https://www.advantisglobal.com/privacy>

1 30. Plaintiff and Class Members have taken reasonable steps to maintain the
2 confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendant
3 to keep their PII confidential and securely maintained, to use this information for necessary
4 purposes only, and to make only authorized disclosures of this information. Plaintiff and Class
5 Members value the confidentiality of their PII and demand security to safeguard their PII.
6

7 31. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff
8 and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep
9 employees' PII safe and confidential.

10 32. Defendant had obligations created by FTC Act, contract, industry standards, and
11 representations made to Plaintiff and Class Members, to keep their PII confidential and to protect
12 it from unauthorized access and disclosure.

13 33. Defendant derived a substantial economic benefit from collecting Plaintiff's and
14 Class Members' PII. Without the required submission of PII , Defendant could not perform the
15 services it provides.
16

17 34. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class
18 Members' PII , Defendant assumed legal and equitable duties and knew or should have known that
19 it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.
20

21 ***The Data Breach***

22 35. On or about December 5, 2023, Defendant, began sending Plaintiff and other Data
23 Breach victims an untitled letter (the "Notice Letter"), informing them that:

24 *What Happened?*

25 On or around October 21, 2022, Advantis Global discovered a security incident that
26 impacted our corporate email system.
27
28

1 What We Are Doing.

2 Upon learning of this issue, we immediately launched a prompt and thorough investigation
3 with the help of external cybersecurity experts experienced in handling these types of
4 incidents. After a thorough and detailed forensic investigation, Advantis determined on
5 November 27, 2023 that resulting from the incident; between August 18, 2022 and October
6 24, 2022, an unauthorized party accessed our corporate email system and/or acquired
7 certain emails containing personal information pertaining to a limited number of
8 individuals. On November 30, 2023, Advantis discovered the most recent contact
9 information of the impacted individuals.

7 What Information Was Involved?

8 The impacted information may have contained some of your personal information,
9 specifically your name, and Social Security number.³

10 36. Omitted from the Notice Letter were the details of the root cause of the Data Breach,
11 the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does
12 not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and
13 Class Members, who retain a vested interest in ensuring that their PII remains protected.

14 37. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with any
15 degree of specificity, Plaintiff and Class Members of the Data Breach’s critical facts. Without these
16 details, Plaintiff’s and Class Members’ ability to mitigate the harms resulting from the Data Breach
17 is severely diminished.

18 38. Defendant did not use reasonable security procedures and practices appropriate to
19 the nature of the sensitive information they were maintaining for Plaintiff and Class Members,
20 causing the exposure of PII, such as encrypting the information or deleting it when it is no longer
21 needed.
22
23

24
25
26 ³ The “Notice Letter”. A sample copy is available at
27 <https://apps.web.maine.gov/online/aewviewer/ME/40/3904cf03-c64e-4719-b5cc-41e56363a10d.shtml>
28

1 39. The attacker accessed and acquired files Defendant shared with a third party
2 containing unencrypted PII of Plaintiff and Class Members, including their Social Security
3 numbers and other sensitive information. Plaintiff's and Class Members' PII was accessed and
4 stolen in the Data Breach.

5
6 40. Plaintiff further believes that her PII and that of Class Members was subsequently
7 sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals
8 that commit cyber-attacks of this type.

9 ***Data Breaches Are Preventable***

10 41. Defendant did not use reasonable security procedures and practices appropriate
11 to the nature of the sensitive information it was maintaining for Plaintiff and Class Members,
12 causing the exposure of PII, such as encrypting the information or deleting it when it is no
13 longer needed.
14

15 42. As explained by the Federal Bureau of Investigation, “[p]revention is the most
16 effective defense against ransomware and it is critical to take precautions for protection.”⁴

17 43. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could
18 and should have implemented, as recommended by the United States Government, the
19 following measures:

- 20
- 21 • Implement an awareness and training program. Because end users are targets,
22 employees and individuals should be aware of the threat of ransomware and how it is
23 delivered.
 - 24 • Enable strong spam filters to prevent phishing emails from reaching the end users and
25 authenticate inbound email using technologies like Sender Policy Framework (SPF),
26 Domain Message Authentication Reporting and Conformance (DMARC), and
27 DomainKeys Identified Mail (DKIM) to prevent email spoofing.

28 ⁴ How to Protect Your Networks from RANSOMWARE, at 3, *available at*:
<https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>

- 1 • Scan all incoming and outgoing emails to detect threats and filter executable files from
2 reaching end users.
- 3 • Configure firewalls to block access to known malicious IP addresses.
- 4 • Patch operating systems, software, and firmware on devices. Consider using a
5 centralized patch management system.
- 6 • Set anti-virus and anti-malware programs to conduct regular scans automatically.
- 7 • Manage the use of privileged accounts based on the principle of least privilege: no users
8 should be assigned administrative access unless absolutely needed; and those with a
9 need for administrator accounts should only use them when necessary.
- 10 • Configure access controls—including file, directory, and network share permissions—
11 with least privilege in mind. If a user only needs to read specific files, the user should
12 not have write access to those files, directories, or shares.
- 13 • Disable macro scripts from office files transmitted via email. Consider using Office
14 Viewer software to open Microsoft Office files transmitted via email instead of full
15 office suite applications.
- 16 • Implement Software Restriction Policies (SRP) or other controls to prevent programs
17 from executing from common ransomware locations, such as temporary folders
18 supporting popular Internet browsers or compression/decompression programs,
19 including the AppData/LocalAppData folder.
- 20 • Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- 21 • Use application whitelisting, which only allows systems to execute programs known
22 and permitted by security policy.
- 23 • Execute operating system environments or specific programs in a virtualized
24 environment.
- 25 • Categorize data based on organizational value and implement physical and logical
26 separation of networks and data for different organizational units.⁵

27 ⁵ *Id.* at 3-4.
28

1 44. To prevent and detect cyber-attacks or ransomware attacks Defendant could and
2 should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team,
3 the following measures:

4 **Secure internet-facing assets**

- 5 - Apply latest security updates
6 - Use threat and vulnerability management
7 - Perform regular audit; remove privileged credentials;

8 **Thoroughly investigate and remediate alerts**

- 9 - Prioritize and treat commodity malware infections as potential full
10 compromise;

11 **Include IT Pros in security discussions**

- 12 - Ensure collaboration among [security operations], [security admins], and
13 [information technology] admins to configure servers and other endpoints
securely;

14 **Build credential hygiene**

- 15 - Use [multifactor authentication] or [network level authentication] and use
16 strong, randomized, just-in-time local admin passwords;

17 **Apply principle of least-privilege**

- 18 - Monitor for adversarial activities
19 - Hunt for brute force attempts
20 - Monitor for cleanup of Event Logs
- Analyze logon events;

21 **Harden infrastructure**

- 22 - Use Windows Defender Firewall
23 - Enable tamper protection
- Enable cloud-delivered protection
24 - Turn on attack surface reduction rules and [Antimalware Scan Interface]
25 for Office [Visual Basic for Applications].⁶

26 ⁶ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at:
27 [https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-
28 preventable-disaster/](https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/)

1
2 45. Given that Defendant was storing the PII of its current and former employees,
3 Defendant could and should have implemented all of the above measures to prevent and detect
4 cyberattacks.

5 46. The occurrence of the Data Breach indicates that Defendant failed to adequately
6 implement one or more of the above measures to prevent cyberattacks, resulting in the Data
7 Breach and the exposure of the PII of more than five thousand current and former employees,
8 including Plaintiff and Class Members.

9
10 ***Defendant Acquires, Collects & Stores Employees' PII***

11 47. Defendant acquires, collects, and stores a massive amount of PII on its employees,
12 former employees, and other personnel.

13 48. As a condition of employment, or as a condition of receiving certain benefits,
14 Defendant requires that employees, former employees, and other personnel entrust it with highly
15 sensitive personal information.

16 49. By obtaining, collecting, and using Plaintiff's and Class Members' PII, Defendant
17 assumed legal and equitable duties and knew or should have known that it was responsible for
18 protecting Plaintiff's and Class Members' PII from disclosure.

19
20 50. Plaintiff and the Class Members have taken reasonable steps to maintain the
21 confidentiality of their PII.

22 51. Plaintiff and the Class Members relied on Defendant to keep their PII confidential
23 and securely maintained, to use this information for business purposes only, and to make only
24 authorized disclosures of this information.

25
26 52. Defendant could have prevented this Data Breach by properly securing and
27 encrypting the files and file servers containing the PII of Plaintiff and Class Members.

1 53. Upon information and belief, Defendant made promises to Plaintiff and Class
2 Members to maintain and protect their PII, demonstrating an understanding of the importance
3 of securing PII.

4 54. Indeed, Defendant provides on its website that: “[w]e strive to protect the security
5 of your personal data by use of appropriate measures and processes.”⁷
6

7 55. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is
8 exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

9 ***Defendant Knew or Should Have Known of the Risk of the Risk Because Employers***
10 ***in Possession of PII are Particularly Susceptable to Cyber Attacks***

11 56. Defendant knew and understood unprotected or exposed PII in the custody of
12 employers, like Defendant, is valuable and highly sought after by nefarious third parties
13 seeking to illegally monetize that PII through unauthorized access.

14 57. Data breaches, including those perpetrated against employers that store PII in
15 their systems, have become widespread.

16 58. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced
17 data breaches, resulting in 66,658,764 individuals' personal information being compromised.⁸
18

19 59. In light of recent high profile data breaches at other industry leading companies,
20 including, Microsoft (250 million records, December 2019), Wattpad (268 million records,
21 June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records,
22 January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3
23 billion records, May 2020), Defendant knew or should have known that the PII that they
24 collected and maintained would be targeted by cybercriminals.
25

26 _____
27 ⁷ <https://www.advantisglobal.com/privacy>

28 ⁸ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>

1 60. Indeed, cyber-attacks, such as the one experienced by Defendant, have become
2 so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have
3 issued a warning to potential targets so they are aware of, and prepared for, a potential attack.
4 As one report explained, smaller entities that store PII are “attractive to ransomware
5 criminals...because they often have lesser IT defenses and a high incentive to regain access to
6 their data quickly.”⁹

7
8 61. At all relevant times, Defendant knew, or reasonably should have known, of the
9 importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable
10 consequences that would occur if Defendant’s data security system was breached, including,
11 specifically, the significant costs that would be imposed on Plaintiff and Class Members as a
12 result of a breach.

13
14 62. Plaintiff and Class Members now face years of constant surveillance of their
15 financial and personal records, monitoring, and loss of rights. The Class is incurring and will
16 continue to incur such damages in addition to any fraudulent use of their PII.

17 63. In the Notice Letter, Defendant makes an offer of 12 months of identity
18 monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as
19 it fails to provide for the fact victims of data breaches and other unauthorized disclosures
20 commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to
21 provide sufficient compensation for the unauthorized release and disclosure of Plaintiff’s and
22 Class Members’ PII.
23

24
25 _____
26 ⁹ https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection
27 ion
28

1 64. Defendant's offer of credit and identity monitoring establishes that Plaintiff's
2 and Class Members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated
3 from Defendant's computer systems.

4 65. The injuries to Plaintiff and Class Members were directly and proximately
5 caused by Defendant's failure to implement or maintain adequate data security measures for
6 the PII of Plaintiff and Class Members.

7 66. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and
8 Class Members are long lasting and severe. Once PII is stolen, particularly Social Security
9 numbers, fraudulent use of that information and damage to victims may continue for years.

10 67. As a business in custody of its current and former employees' PII, Defendant
11 knew, or should have known, the importance of safeguarding PII entrusted to them by Plaintiff
12 and Class Members, and of the foreseeable consequences if its data security systems were
13 breached. This includes the significant costs imposed on Plaintiff and Class Members as a
14 result of a breach. Defendant failed, however, to take adequate cybersecurity measures to
15 prevent the Data Breach.
16

17
18 ***Value of Personally Identifiable Information***

19 68. The Federal Trade Commission ("FTC") defines identity theft as "a fraud
20 committed or attempted using the identifying information of another person without
21 authority."¹⁰ The FTC describes "identifying information" as "any name or number that may
22 be used, alone or in conjunction with any other information, to identify a specific person,"
23 including, among other things, "[n]ame, Social Security number, date of birth, official State or
24

25
26
27

28 ¹⁰ 17 C.F.R. § 248.201 (2013).

1 government issued driver’s license or identification number, alien registration number,
2 government passport number, employer or taxpayer identification number.”¹¹

3 69. The PII of individuals remains of high value to criminals, as evidenced by the
4 prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen
5 identity credentials.¹²

6 70. For example, Personal Information can be sold at a price ranging from \$40 to
7 \$200, and bank details have a price range of \$50 to \$200.¹³

8 71. Criminals can also purchase access to entire company data breaches from \$900
9 to \$4,500.¹⁴

10 72. Social Security numbers, which were compromised for some of the Class
11 Members as alleged herein, for example, are among the worst kind of PII to have stolen because
12 they may be put to a variety of fraudulent uses and are difficult for an individual to change.
13 The Social Security Administration stresses that the loss of an individual’s Social Security
14 number, as is the case here, can lead to identity theft and extensive financial fraud:
15
16

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

22 ¹¹ *Id.*

23 ¹² *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct.
24 16, 2019, available at: [https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-
web-how-much-it-costs/](https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/)

25 ¹³ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6,
26 2017, available at: [https://www.experian.com/blogs/ask-experian/heres-how-much-your-
personal-information-is-selling-for-on-the-dark-web/](https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/)

27 ¹⁴ *In the Dark*, VPNOverview, 2019, available at: [https://vpnoverview.com/privacy/anonymous-
browsing/in-the-dark/](https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/)

1 illegally using your Social Security number and assuming your identity can cause
2 a lot of problems.¹⁵

3 73. What’s more, it is no easy task to change or cancel a stolen Social Security
4 number. An individual cannot obtain a new Social Security number without significant
5 paperwork and evidence of actual misuse. In other words, preventive action to defend against
6 the possibility of misuse of a Social Security number is not permitted; an individual must show
7 evidence of actual, ongoing fraud activity to obtain a new number.

8 74. Even then, a new Social Security number may not be effective. According to
9 Julie Ferguson of the Identity Theft Resource Center, “[t]he credit bureaus and banks are able
10 to link the new number very quickly to the old number, so all of that old bad information is
11 quickly inherited into the new Social Security number.”¹⁶

13 75. Based on the foregoing, the information compromised in the Data Breach is
14 significantly more valuable than the loss of, for example, credit card information in a retailer
15 data breach because, there, victims can cancel or close credit and debit card accounts. The
16 information compromised in this Data Breach is impossible to “close” and difficult, if not
17 impossible, to change—Social Security numbers and names.

19 76. This data demands a much higher price on the black market. Martin Walter,
20 senior director at cybersecurity firm RedSeal, explained, “Compared to credit card
21
22
23

24 _____
25 ¹⁵ Social Security Administration, *Identity Theft and Your Social Security Number*, available at:
<https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Oct. 17, 2022).

26 ¹⁶ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR
27 (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft>
28

1 information, personally identifiable information and Social Security numbers are worth more
2 than 10x on the black market.”¹⁷

3 77. Among other forms of fraud, identity thieves may obtain driver’s licenses,
4 government benefits, medical services, and housing or even give false information to police.

5 78. The fraudulent activity resulting from the Data Breach may not come to light
6 for years. There may be a time lag between when harm occurs versus when it is discovered,
7 and also between when PII is stolen and when it is used. According to the U.S. Government
8 Accountability Office (“GAO”), which conducted a study regarding data breaches:
9

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

15 ***Defendant Fails to Comply with FTC Guidelines***

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

20 80. In 2016, the FTC updated its publication, Protecting Personal Information: A
21 Guide for Business, which established cyber-security guidelines for businesses. These
22 guidelines note that businesses should protect the personal employee information that they
23

24 ¹⁷ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*
25 *Numbers*, IT World, (Feb. 6, 2015), available at:
26 <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>

27 ¹⁸ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:
28 <https://www.gao.gov/assets/gao-07-737.pdf>

1 keep; properly dispose of personal information that is no longer needed; encrypt information
2 stored on computer networks; understand their network's vulnerabilities; and implement
3 policies to correct any security problems.¹⁹

4 81. The guidelines also recommend that businesses use an intrusion detection
5 system to expose a breach as soon as it occurs; monitor all incoming traffic for activity
6 indicating someone is attempting to hack the system; watch for large amounts of data being
7 transmitted from the system; and have a response plan ready in the event of a breach.²⁰

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

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

22 84. These FTC enforcement actions include actions against employers over the
23 compromised PII of its employees, like Defendant here.

25 ¹⁹ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).
26 Available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-
27 personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)

28 ²⁰ *Id.*

1 85. Defendant failed to properly implement basic data security practices.

2 86. Defendant's failure to employ reasonable and appropriate measures to protect
3 against unauthorized access to employees' PII constitutes an unfair act or practice prohibited
4 by Section 5 of the FTC Act, 15 U.S.C. § 45.

5 87. Upon information and belief, Defendant was at all times fully aware of its
6 obligation to protect the PII of its employees. Defendant was also aware of the significant
7 repercussions that would result from its failure to do so.

8
9 ***Defendant Fails to Comply with Industry Standards***

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

13 89. Several best practices have been identified that a minimum should be
14 implemented by employers in possession of PII, like Defendant, including but not limited to:
15 educating all employees; strong passwords; multi-layer security, including firewalls, anti-
16 virus, and anti-malware software; encryption, making data unreadable without a key; multi-
17 factor authentication; backup data and limiting which employees can access sensitive data.
18 Defendant failed to follow these industry best practices, including a failure to implement multi-
19 factor authentication.
20

21 90. Other best cybersecurity practices that are standard for employers include
22 installing appropriate malware detection software; monitoring and limiting the network ports;
23 protecting web browsers and email management systems; setting up network systems such as
24 firewalls, switches and routers; monitoring and protection of physical security systems;
25
26
27
28

1 protection against any possible communication system; training staff regarding critical points.
2 Defendant failed to follow these cybersecurity best practices, including failure to train staff.

3 91. Defendant failed to meet the minimum standards of any of the following
4 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation
5 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,
6 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
7 for Internet Security's Critical Security Controls (CIS CSC), which are all established
8 standards in reasonable cybersecurity readiness.
9

10 92. These foregoing frameworks are existing and applicable industry standards for
11 an employer's obligations to its employees with respect to data privacy. Upon information
12 and belief, Defendant failed to comply with at least one—or all—of these accepted standards,
13 thereby opening the door to the threat actor and causing the Data Breach.
14

15 ***Common Injuries and Damages***

16 93. As a result of Defendant's ineffective and inadequate data security practices, the
17 Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals,
18 the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent,
19 and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i)
20 invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time
21 and opportunity costs associated with attempting to mitigate the actual consequences of the
22 Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual
23 consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the
24 continued and certainly increased risk to their PII, which: (a) remains unencrypted and
25 available for unauthorized third parties to access and abuse; and (b) remains backed up in
26
27
28

1 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant
2 fails to undertake appropriate and adequate measures to protect the PII.

3 ***The Data Breach Increases Plaintiff's and Class Member's Risk of Identity Theft***

4 94. Plaintiff and Class Members are at a present and continued risk of identity theft
5 for years to come.

6 95. The unencrypted PII of Plaintiff and Class Members has or will be available for
7 sale on the dark web because that is the *modus operandi* of hackers.

8 96. In addition, unencrypted PII may fall into the hands of companies that will use
9 the detailed PII for targeted marketing without the approval of Plaintiff and Class Members.

10 97. Unauthorized individuals can easily access the PII of Plaintiff and Class
11 Members.

12 98. The link between a data breach and the risk of identity theft is simple and well
13 established. Criminals acquire and steal PII to monetize the information. Criminals monetize
14 the data by selling the stolen information on the black market to other criminals who then
15 utilize the information to commit a variety of identity theft related crimes discussed below.

16 99. Because a person's identity is akin to a puzzle with multiple data points, the
17 more accurate pieces of data an identity thief obtains about a person, the easier it is for the
18 thief to take on the victim's identity--or track the victim to attempt other hacking crimes against
19 the individual to obtain more data to perfect a crime.

20 100. For example, armed with just a name and date of birth, a data thief can utilize a
21 hacking technique referred to as "social engineering" to obtain even more information about a
22 victim's identity, such as a person's login credentials or Social Security number. Social
23 engineering is a form of hacking whereby a data thief uses previously acquired information to
24
25
26
27
28

1 manipulate and trick individuals into disclosing additional confidential or personal information
2 through means such as spam phone calls and text messages or phishing emails. Data Breaches
3 can be the starting point for these additional targeted attacks on the victims.

4 101. One such example of criminals piecing together bits and pieces of compromised
5 PII for profit is the development of “Fullz” packages.²¹

6 102. With “Fullz” packages, cyber-criminals can cross-reference two sources of PII
7 to marry unregulated data available elsewhere to criminally stolen data with an astonishingly
8 complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

9 103. The development of “Fullz” packages means here that the stolen PII from the
10 Data Breach can easily be used to link and identify it to Plaintiff’s and Class Members’ phone
11 numbers, email addresses, and other unregulated sources and identifiers. In other words, even
12 if certain information such as emails, phone numbers, or credit card numbers may not be
13 included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a
14 Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as
15 illegal and scam telemarketers) over and over.

16
17
18
19 ²¹ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not
20 limited to, the name, address, credit card information, social security number, date of birth, and
21 more. As a rule of thumb, the more information you have on a victim, the more money that can be
22 made off of those credentials. Fullz are usually pricier than standard credit card credentials,
23 commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning
24 credentials into money) in various ways, including performing bank transactions over the phone
25 with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials
26 associated with credit cards that are no longer valid, can still be used for numerous purposes,
27 including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule
28 account” (an account that will accept a fraudulent money transfer from a compromised account)
without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground*
Stolen From Texas Life Insurance Firm, Krebs on Security (Sep. 18, 2014),
[https://krebsonsecuriv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-](https://krebsonsecuriv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-)
[texas-life-insurance-\]\(https://krebsonsecuriv.com/2014/09/medical-records-for-sale-in-](https://krebsonsecuriv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/)
[underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecuriv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/)

1 104. The existence and prevalence of “Fullz” packages means that the PII stolen from
2 the data breach can easily be linked to the unregulated data (like driver's license numbers) of
3 Plaintiff and the other Class Members.

4 105. Thus, even if certain information (such as driver's license numbers) was not
5 stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.
6

7 106. Then, this comprehensive dossier can be sold—and then resold in perpetuity—
8 to crooked operators and other criminals (like illegal and scam telemarketers).

9 ***Loss of Time to Mitigate the Risk of Identity Theft and Fraud***

10 107. As a result of the recognized risk of identity theft, when a Data Breach occurs,
11 and an individual is notified by a company that their PII was compromised, as in this Data
12 Breach, the reasonable person is expected to take steps and spend time to address the dangerous
13 situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of
14 identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports
15 could expose the individual to greater financial harm – yet, the resource and asset of time has
16 been lost.
17

18 108. Thus, due to the actual and imminent risk of identity theft that Plaintiff and Class
19 Members face, Defendant’s Notice Letter instructs Plaintiff and Class Members to do the
20 following: “you should always remain vigilant in reviewing your financial account statements
21 and credit reports for fraudulent or irregular activity on a regular basis.”²²
22

23 109. Plaintiff and Class Members have spent, and will spend additional time in the
24 future, on a variety of prudent actions, such as researching and verifying the legitimacy of the
25 Data Breach, replacing impacted debit and/or credit cards, changing their phone numbers,
26

27 ²² Notice Letter.
28

1 closing impacted bank accounts, changing passwords and resecuring their own computer
2 networks, and contacting financial institutions to sort out fraudulent activity on their accounts.

3 110. Plaintiff's mitigation efforts are consistent with the U.S. Government
4 Accountability Office that released a report in 2007 regarding data breaches ("GAO Report")
5 in which it noted that victims of identity theft will face "substantial costs and time to repair
6 the damage to their good name and credit record."²³

7
8 111. Plaintiff's mitigation efforts are also consistent with the steps that FTC
9 recommends that data breach victims take several steps to protect their personal and financial
10 information after a data breach, including: contacting one of the credit bureaus to place a fraud
11 alert (consider an extended fraud alert that lasts for seven years if someone steals their
12 identity), reviewing their credit reports, contacting companies to remove fraudulent charges
13 from their accounts, placing a credit freeze on their credit, and correcting their credit reports.²⁴

14
15 112. And for those Class Members who experience actual identity theft and fraud,
16 the United States Government Accountability Office released a report in 2007 regarding data
17 breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial
18 costs and time to repair the damage to their good name and credit record."²⁵

19
20
21
22
23

24 ²³ See United States Government Accountability Office, GAO-07-737, Personal Information: Data
Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full
Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

25 ²⁴ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

26 ²⁵ See "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited;
27 However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007,
<https://www.gao.gov/new.items/d07737.pdf> ("GAO Report").

Diminution Value of PII

113. PII is a valuable property right.²⁶ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

114. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other entities in custody of PII often purchase PII on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims herself. Insurance companies purchase and use wrongfully disclosed PII to adjust their insureds' medical insurance premiums.

115. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.²⁷ In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{28,29}

116. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.³⁰

²⁶ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

²⁷ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

²⁸ <https://datacoup.com/>

²⁹ <https://digi.me/what-is-digime/>

³⁰ Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html>

1 117. Sensitive PII can sell for as much as \$363 per record according to the Infosec
2 Institute.³¹

3 118. As a result of the Data Breach, Plaintiff’s and Class Members’ PII, which has
4 an inherent market value in both legitimate and dark markets, has been damaged and
5 diminished by its compromise and unauthorized release. However, this transfer of value
6 occurred without any consideration paid to Plaintiff or Class Members for their property,
7 resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the
8 Data has been lost, thereby causing additional loss of value.

9 119. Based on the foregoing, the information compromised in the Data Breach is
10 significantly more valuable than the loss of, for example, credit card information in a retailer
11 data breach because, there, victims can cancel or close credit and debit card accounts. The
12 information compromised in this Data Breach is impossible to “close” and difficult, if not
13 impossible, to change, e.g., Social Security numbers and names.

14 120. Among other forms of fraud, identity thieves may obtain driver’s licenses,
15 government benefits, medical services, and housing or even give false information to police.

16 121. The fraudulent activity resulting from the Data Breach may not come to light
17 for years.

18 122. At all relevant times, Defendant knew, or reasonably should have known, of the
19 importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable
20 consequences that would occur if Defendant’s data security system was breached, including,
21
22
23
24
25

26
27 ³¹ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015),
28 <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

1 specifically, the significant costs that would be imposed on Plaintiff and Class Members as a
2 result of a breach.

3 123. Plaintiff and Class Members now face years of constant surveillance of their
4 financial and personal records, monitoring, and loss of rights. The Class is incurring and will
5 continue to incur such damages in addition to any fraudulent use of their PII.
6

7 124. Defendant was, or should have been, fully aware of the unique type and the
8 significant volume of data on Defendant's network, amounting to more than five thousand
9 individuals' detailed personal information and, thus, the significant number of individuals who
10 would be harmed by the exposure of the unencrypted data.

11 125. The injuries to Plaintiff and Class Members were directly and proximately
12 caused by Defendant's failure to implement or maintain adequate data security measures for
13 the PII of Plaintiff and Class Members.
14

15 ***Future Costs of Credit and Identity Theft Monitoring is Reasonable and Necessary***

16 126. Given the type of targeted attack in this case and sophisticated criminal activity,
17 the type of PII involved, and the volume of PII accessed in the Data Breach, there is a strong
18 probability that entire batches of stolen information have been placed, or will be placed, on the
19 black market/dark web for sale and purchase by criminals intending to utilize the PII for
20 identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or
21 to launder money; file false tax returns; take out loans or lines of credit; or file false
22 unemployment claims.
23

24 127. Such fraud may go undetected until debt collection calls commence months, or
25 even years, later.
26
27
28

1 128. An individual may not know that his or her Social Security Number was used to
2 file for unemployment benefits until law enforcement notifies the individual’s employer of the
3 suspected fraud. Fraudulent tax returns are typically discovered only when an individual’s
4 authentic tax return is rejected.

5
6 129. Furthermore, the information accessed and disseminated in the Data Breach is
7 significantly more valuable than the loss of, for example, credit card information in a retailer
8 data breach, where victims can easily cancel or close credit and debit card accounts.³² The
9 information disclosed in this Data Breach is impossible to “close” and difficult, if not
10 impossible, to change (such as Social Security numbers).

11 130. Consequently, Plaintiff and Class Members are at a present and continuous risk
12 of fraud and identity theft for many years into the future.

13
14 131. The retail cost of credit monitoring and identity theft monitoring can cost around
15 \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect
16 Class Members from the risk of identity theft that arose from Defendant’s Data Breach.

17 ***Loss of Benefit of the Bargain***

18 132. Furthermore, Defendant’s poor data security deprived Plaintiff and Class
19 Members of the benefit of their bargain. When agreeing to obtain employment at Defendant
20 under certain terms, Plaintiff and other reasonable employees understood and expected that
21 Defendant would properly safeguard and protect their PII, when in fact, Defendant did not
22 provide the expected data security. Accordingly, Plaintiff and Class Members received
23
24
25

26 ³² See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*,
27 FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.
28

1 employment positions of a lesser value than what they reasonably expected to receive under
2 the bargains they struck with Defendant.

3 ***Plaintiff Kristianne Scott's Experience***

4 133. Plaintiff Scott is a former employee at Advantis who worked there from
5 approximately 2022 to 2023.
6

7 134. As a condition of her employment at Advantis, she was required to supply
8 Defendant with her PII, including but not limited to her name and Social Security number.

9 135. Plaintiff Scott is very careful about sharing her sensitive PII. Plaintiff stores any
10 documents containing her PII in a safe and secure location. She has never knowingly
11 transmitted unencrypted sensitive PII over the internet or any other unsecured source.
12

13 136. At the time of the Data Breach—between August 18, 2022 and October 24,
14 2022—Defendant retained Plaintiff's PII in its system.

15 137. Plaintiff Scott received the Notice Letter, by U.S. mail, directly from Defendant,
16 dated December 5, 2023. According to the Notice Letter, Plaintiff's PII was improperly
17 accessed and obtained by unauthorized third parties, including her full name and Social
18 Security number.

19 138. As a result of the Data Breach, and at the direction of Defendant's Notice Letter,
20 which instructs Plaintiff to "remain vigilant in reviewing your financial account statements
21 and credit reports for fraudulent or irregular activity on a regular basis[,]”³³ Plaintiff made
22 reasonable efforts to mitigate the impact of the Data Breach, including but not limited to:
23 researching and verifying the legitimacy of the Data Breach, replacing impacted debit cards,
24 changing her phone number, closing impacted bank accounts, changing passwords and
25

26
27

³³ Notice Letter.
28

1 resecuring her own computer network, and contacting financial institutions to sort out
2 fraudulent activity on her accounts. Plaintiff have spent significant on mitigation activities in
3 response to the Data Breach--valuable time Plaintiff otherwise would have spent on other
4 activities, including but not limited to work and/or recreation. This time has been lost forever
5 and cannot be recaptured.

6
7 139. Subsequent to the Data Breach, Plaintiff Scott has suffered numerous,
8 substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of her PII;
9 (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with
10 attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs
11 associated with attempting to mitigate the actual consequences of the Data Breach; (vi)
12 statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk
13 to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access
14 and abuse; and (b) remains backed up in Defendant's possession and is subject to further
15 unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate
16 measures to protect the PII.

17
18 140. Plaintiff also suffered actual injury in the form of experiencing an increase in spam
19 calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

20
21 141. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has
22 been compounded by the fact that Defendant has still not fully informed her of key details about
23 the Data Breach's occurrence.

24 142. As a result of the Data Breach, Plaintiff anticipates spending considerable time and
25 money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

1 143. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be
2 at increased risk of identity theft and fraud for years to come.

3 144. Plaintiff Scott has a continuing interest in ensuring that her PII, which, upon
4 information and belief, remains backed up in Defendant's possession, is protected and safeguarded
5 from future breaches.
6

7 CLASS ACTION ALLEGATIONS

8 145. Plaintiff brings this action on behalf of herself and on behalf of all other persons
9 similarly situated.

10 146. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff proposes the following
11 Class definitions, subject to amendment as appropriate:
12

13 **Nationwide Class**

14 All individuals in the United States whose PII was impacted as a result of the Data Breach
announced by Defendant in December 2023 (the "Class").

15 **Michigan Subclass**

16 All individuals in the state of Michigan whose PII was impacted as a result of the Data
Breach announced by Defendant in December 2023 (the "Michigan Subclass").

17 147. Excluded from the Classes are Defendant's officers and directors, and any entity in
18 which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys,
19 successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the
20 judiciary to whom this case is assigned, their families and members of their staff.
21

22 148. Plaintiff hereby reserve the right to amend or modify the Class and/or Michigan
23 Subclass definition with greater specificity or division after having had an opportunity to conduct
24 discovery.

25 149. Numerosity. The Members of the Class are so numerous that joinder of all of them
26 is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time,
27
28

1 according to the reports submitted to the Maine Attorney General, the Class consists of
2 approximately 5,000 individuals whose data was compromised in Data Breach.³⁴

3 150. Commonality. There are questions of law and fact common to the Class, which
4 predominate over any questions affecting only individual Class Members. These common
5 questions of law and fact include, without limitation:
6

- 7 a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's
8 and Class Members' PII;
- 9 b. Whether Defendant failed to implement and maintain reasonable security
10 procedures and practices appropriate to the nature and scope of the information
11 compromised in the Data Breach;
- 12 c. Whether Defendant's data security systems prior to and during the Data Breach
13 complied with applicable data security laws and regulations;
- 14 d. Whether Defendant's data security systems prior to and during the Data Breach
15 were consistent with industry standards;
- 16 e. Whether Defendant owed a duty to Class Members to safeguard their PII;
- 17 f. Whether Defendant breached its duty to Class Members to safeguard their PII;
- 18 g. Whether computer hackers obtained Class Members' PII in the Data Breach;
- 19 h. Whether Defendant knew or should have known that its data security systems
20 and monitoring processes were deficient;
- 21 i. Whether Plaintiff and Class Members suffered legally cognizable damages as
22 a result of Defendant's misconduct;
- 23
- 24
- 25
- 26

27 ³⁴ <https://apps.web.maine.gov/online/aeviewer/ME/40/3904cf03-c64e-4719-b5cc-41e56363a10d.shtml>

- 1 j. Whether Defendant's conduct was negligent;
- 2 k. Whether Defendant breached implied contracts for adequate data security with
- 3 Plaintiff and Class Members;
- 4 l. Whether Defendant was unjustly enriched by retention of the monetary benefits
- 5 conferred on it by Plaintiff and Class Members;
- 6 m. Whether Defendant failed to provide notice of the Data Breach in a timely
- 7 manner; and,
- 8 n. Whether Plaintiff and Class Members are entitled to damages, civil penalties,
- 9 punitive damages, and/or injunctive relief.
- 10

11 151. Typicality. Plaintiff's claims are typical of those of other Class Members because

12 Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

13 152. Adequacy of Representation. Plaintiff will fairly and adequately represent and

14 protect the interests of the Members of the Class. Plaintiff's Counsel are competent and

15 experienced in litigating class actions.

16 153. Predominance. Defendant has engaged in a common course of conduct toward

17 Plaintiff and Class Members, in that all the Plaintiff's and Class Members' PII was stored on the

18 same computer systems and unlawfully accessed in the same way. The common issues arising

19 from Defendant's conduct affecting Class Members set out above predominate over any

20 individualized issues. Adjudication of these common issues in a single action has important and

21 desirable advantages of judicial economy.

22 154. Superiority. A class action is superior to other available methods for the fair and

23 efficient adjudication of the controversy. Class treatment of common questions of law and fact is

24 superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class

25

26

27

28

1 Members would likely find that the cost of litigating their individual claims is prohibitively high
2 and would therefore have no effective remedy. The prosecution of separate actions by individual
3 Class Members would create a risk of inconsistent or varying adjudications with respect to
4 individual Class Members, which would establish incompatible standards of conduct for
5 Defendant. In contrast, the conduct of this action as a class action presents far fewer management
6 difficulties, conserves judicial resources and the parties' resources, and protects the rights of each
7 Class Member.
8 Class Member.

9 155. Defendant has acted on grounds that apply generally to the Class as a whole, so that
10 class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-
11 wide basis.

12 156. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for
13 certification because such claims present only particular, common issues, the resolution of which
14 would advance the disposition of this matter and the parties' interests therein. Such particular
15 issues include, but are not limited to:
16

- 17 a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due
18 care in collecting, storing, and safeguarding their PII;
- 19 b. Whether Defendant's security measures to protect its data systems were
20 reasonable in light of best practices recommended by data security experts;
- 21 c. Whether Defendant's failure to institute adequate protective security measures
22 amounted to negligence;
- 23 d. Whether Defendant failed to take commercially reasonable steps to safeguard
24 consumer PII; and
25
26
27
28

1 e. Whether adherence to FTC data security recommendations, and measures
2 recommended by data security experts would have reasonably prevented the
3 Data Breach.

4 157. Finally, all Members of the proposed Class are readily ascertainable. Defendant has
5 access to Class Members' names and addresses affected by the Data Breach. Class Members have
6 already been preliminarily identified and sent Notice of the Data Breach by Defendant.
7

8 **COUNT I**
9 **Negligence**
10 **(On behalf of Plaintiff and the Class)**

11 158. Plaintiff re-alleges and incorporates the above allegations as if fully set forth
12 herein.

13 159. Defendant requires its employees, including Plaintiff and Class Members, to
14 submit non-public PII in the ordinary course of providing its services.

15 160. Defendant gathered and stored the PII of Plaintiff and Class Members as part of
16 its business of soliciting its employees, which solicitations and services affect commerce.

17 161. Plaintiff and Class Members entrusted Defendant with their PII with the
18 understanding that Defendant would safeguard their information.

19 162. Defendant had full knowledge of the sensitivity of the PII and the types of harm
20 that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.
21

22 163. By assuming the responsibility to collect and store this data, and in fact doing
23 so, and sharing it and using it for commercial gain, Defendant had a duty of care to use
24 reasonable means to secure and to prevent disclosure of the information, and to safeguard the
25 information from theft.
26
27
28

1 164. Defendant had a duty to employ reasonable security measures under Section 5
2 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in
3 or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice
4 of failing to use reasonable measures to protect confidential data.
5

6 165. Defendant owed a duty of care to Plaintiff and Class Members to provide data
7 security consistent with industry standards and other requirements discussed herein, and to
8 ensure that its systems and networks, and the personnel responsible for them, adequately
9 protected the PII.

10 166. Defendant's duty of care to use reasonable security measures arose as a result of
11 the special relationship that existed between Defendant and Plaintiff and Class Members. That
12 special relationship arose because Plaintiff and the Class entrusted Defendant with their
13 confidential PII, a necessary part of obtaining employment at Defendant.
14

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

18 168. Defendant was subject to an “independent duty,” untethered to any contract
19 between Defendant and Plaintiff or the Class.
20

21 169. Defendant also had a duty to exercise appropriate clearinghouse practices to
22 remove former employees’ ’ PII it was no longer required to retain pursuant to regulations.

23 170. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and
24 the Class of the Data Breach.

25 171. Defendant had and continues to have a duty to adequately disclose that the PII
26 of Plaintiff and the Class within Defendant’s possession might have been compromised, how
27
28

1 it was compromised, and precisely the types of data that were compromised and when. Such
2 notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and
3 repair any identity theft and the fraudulent use of their PII by third parties.

4 172. Defendant breached its duties, pursuant to the FTC Act and other applicable
5 standards, and thus was negligent, by failing to use reasonable measures to protect Class
6 Members' PII. The specific negligent acts and omissions committed by Defendant include, but
7 are not limited to, the following:
8

- 9 a. Failing to adopt, implement, and maintain adequate security measures to
10 safeguard Class Members' PII;
- 11 b. Failing to adequately monitor the security of their networks and systems;
- 12 c. Allowing unauthorized access to Class Members' PII;
- 13 d. Failing to detect in a timely manner that Class Members' PII had been
14 compromised;
- 15 e. Failing to remove former employees' PII it was no longer required to retain
16 pursuant to regulations,
- 17 f. Failing to timely and adequately notify Class Members about the Data Breach's
18 occurrence and scope, so that they could take appropriate steps to mitigate the
19 potential for identity theft and other damages; and
- 20 g. Failing to secure its stand-alone personal computers, such as the reception desk
21 computers, even after discovery of the data breach.

22 173. Defendant violated Section 5 of the FTC Act by failing to use reasonable
23 measures to protect PII and not complying with applicable industry standards, as described in
24 detail herein. Defendant's conduct was particularly unreasonable given the nature and amount
25
26
27
28

1 of PII it obtained and stored and the foreseeable consequences of the immense damages that
2 would result to Plaintiff and the Class.

3 174. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

4 175. Plaintiff and Class Members were within the class of persons the Federal Trade
5 Commission Act was intended to protect and the type of harm that resulted from the Data
6 Breach was the type of harm the statute was intended to guard against.
7

8 176. The FTC has pursued enforcement actions against businesses, which, as a result
9 of their failure to employ reasonable data security measures and avoid unfair and deceptive
10 practices, caused the same harm as that suffered by Plaintiff and the Class.

11 177. A breach of security, unauthorized access, and resulting injury to Plaintiff and
12 the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security
13 practices.
14

15 178. It was foreseeable that Defendant's failure to use reasonable measures to protect
16 Class Members' PII would result in injury to Class Members. Further, the breach of security
17 was reasonably foreseeable given the known high frequency of cyberattacks and data breaches
18 targeting employers in possession of PII.

19 179. Defendant has full knowledge of the sensitivity of the PII and the types of harm
20 that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.
21

22 180. Plaintiff and the Class were the foreseeable and probable victims of any
23 inadequate security practices and procedures. Defendant knew or should have known of the
24 inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance
25 of providing adequate security of that PII, and the necessity for encrypting PII stored on
26 Defendant's systems.
27
28

1 181. It was therefore foreseeable that the failure to adequately safeguard Class
2 Members' PII would result in one or more types of injuries to Class Members.

3 182. Plaintiff and the Class had no ability to protect their PII that was in, and possibly
4 remains in, Defendant's possession.

5 183. Defendant was in a position to protect against the harm suffered by Plaintiff and
6 the Class as a result of the Data Breach.

7 184. Defendant's duty extended to protecting Plaintiff and the Class from the risk of
8 foreseeable criminal conduct of third parties, which has been recognized in situations where
9 the actor's own conduct or misconduct exposes another to the risk or defeats protections put
10 in place to guard against the risk, or where the parties are in a special relationship. *See*
11 Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized
12 the existence of a specific duty to reasonably safeguard personal information.
13

14 185. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully
15 lost and disclosed to unauthorized third persons as a result of the Data Breach.
16

17 186. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff
18 and the Class, the PII of Plaintiff and the Class would not have been compromised.

19 187. There is a close causal connection between Defendant's failure to implement
20 security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent
21 harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and
22 accessed as the proximate result of Defendant's failure to exercise reasonable care in
23 safeguarding such PII by adopting, implementing, and maintaining appropriate security
24 measures.
25
26
27
28

1 188. As a direct and proximate result of Defendant’s negligence, Plaintiff and the Class
2 have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft
3 of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated
4 with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the
5 bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences
6 of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii)
7 statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to
8 their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and
9 abuse; and (b) remains backed up in Defendant’s possession and is subject to further unauthorized
10 disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect
11 the PII.
12

13 189. As a direct and proximate result of Defendant’s negligence, Plaintiff and the
14 Class have suffered and will continue to suffer other forms of injury and/or harm, including,
15 but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-
16 economic losses.
17

18 190. Additionally, as a direct and proximate result of Defendant’s negligence,
19 Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their
20 PII, which remain in Defendant’s possession and is subject to further unauthorized disclosures
21 so long as Defendant fails to undertake appropriate and adequate measures to protect the PII
22 in its continued possession.
23

24 191. Plaintiff and Class Members are entitled to compensatory and consequential
25 damages suffered as a result of the Data Breach.
26
27
28

1 192. Defendant’s negligent conduct is ongoing, in that it still holds the PII of Plaintiff
2 and Class Members in an unsafe and insecure manner.

3 193. Plaintiff and Class Members are also entitled to injunctive relief requiring
4 Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to
5 future annual audits of those systems and monitoring procedures; and (iii) continue to provide
6 adequate credit monitoring to all Class Members.
7

8 **COUNT II**
9 **Negligence *Per Se***
10 **(On Behalf of Plaintiff and the Class)**

11 194. Plaintiff re-alleges and incorporates the above allegations as if fully set forth
12 herein.

13 195. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or
14 affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice
15 by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and
16 orders also form the basis of Defendant’s duty.

17 196. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing
18 to use reasonable measures to protect PII and not complying with industry standards. Defendant’s
19 conduct was particularly unreasonable given the nature and amount of PII obtained and stored and
20 the foreseeable consequences of a data breach on Defendant’s systems.

21 197. Defendant’s violation of Section 5 of the FTC Act (and similar state statutes)
22 constitutes negligence *per se*.

23 198. Class members are consumers within the class of persons Section 5 of the FTC Act
24 (and similar state statutes) were intended to protect.
25
26
27
28

1 203. Plaintiff and Class Members were required to provide their PII to Defendant as
2 a condition of obtaining employment at Defendant.

3 204. Plaintiff and the Class entrusted their PII to Defendant. In so doing, Plaintiff
4 and the Class entered into implied contracts with Defendant by which Defendant agreed to
5 safeguard and protect such information, to keep such information secure and confidential, and
6 to timely and accurately notify Plaintiff and the Class if their data had been breached and
7 compromised or stolen.
8

9 205. In entering into such implied contracts, Plaintiff and Class Members reasonably
10 believed and expected that Defendant's data security practices complied with relevant laws
11 and regulations and were consistent with industry standards.
12

13 206. Implicit in the agreement between Plaintiff and Class Members and the
14 Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes
15 only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of
16 the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and
17 all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII
18 of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only
19 under conditions that kept such information secure and confidential.
20

21 207. The mutual understanding and intent of Plaintiff and Class Members on the one
22 hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

23 208. Defendant solicited, offered, and invited Plaintiff and Class Members to provide
24 their PII as part of Defendant's regular business practices. Plaintiff and Class Members
25 accepted Defendant's offers and provided their PII to Defendant.
26
27
28

1 209. In accepting the PII of Plaintiff and Class Members, Defendant understood and
2 agreed that it was required to reasonably safeguard the PII from unauthorized access or
3 disclosure.

4 210. On information and belief, at all relevant times Defendant promulgated,
5 adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and
6 Class Members that it would only disclose PII under certain circumstances, none of which
7 relate to the Data Breach.
8

9 211. On information and belief, Defendant further promised to comply with industry
10 standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

11 212. Plaintiff and Class Members provided their labor and PII to Defendant with the
12 reasonable belief and expectation that Defendant would use part of its earnings to obtain
13 adequate data security. Defendant failed to do so.
14

15 213. Plaintiff and Class Members would not have entrusted their PII to Defendant in
16 the absence of the implied contract between them and Defendant to keep their information
17 reasonably secure.

18 214. Plaintiff and Class Members would not have entrusted their PII to Defendant in
19 the absence of their implied promise to monitor their computer systems and networks to ensure
20 that it adopted reasonable data security measures.
21

22 215. Plaintiff and Class Members fully and adequately performed their obligations
23 under the implied contracts with Defendant.

24 216. Defendant breached the implied contracts it made with Plaintiff and the Class
25 by failing to safeguard and protect their personal information, by failing to delete the
26 information of Plaintiff and the Class once the relationship ended, and by failing to provide
27
28

1 223. The intrusion was into a place or thing which was private and is entitled to be
2 private, in that Plaintiff and the Class Members provided and disclosed their PII to Defendant
3 privately with an intention that the PII would be kept confidential and protected from
4 unauthorized disclosure. Plaintiff and the Class Members were reasonable to believe that such
5 information would be kept private and would not be disclosed without their written
6 authorization.
7

8 224. As a direct and proximate result of Defendant's above acts, Plaintiff's and the
9 Class Members' PII was viewed, distributed, and used by persons without prior written
10 authorization and Plaintiff and the Class Members suffered damages as described herein.
11

12 225. Defendant has committed oppression, fraud, or malice by permitting the
13 unauthorized disclosure of Plaintiff's and the Class Members' PII with a willful and conscious
14 disregard of Plaintiff's and the Class Members' right to privacy.

15 226. Plaintiff and Class Members have no adequate remedy at law for the injuries in
16 that a judgment for the monetary damages will not end the invasion of privacy for Plaintiff and
17 the Class, and Defendant may freely treat Plaintiff's and Class Members' PII with sub-standard
18 and insufficient protections.

19 227. Unless and until enjoined, and restrained by order of this Court, Defendant's
20 wrongful conduct will continue to cause Plaintiff and the Class Members great and irreparable
21 injury in that the PII maintained by Defendant can be viewed, printed, distributed, and used by
22 unauthorized persons.
23
24
25
26
27
28

COUNT V

**Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.* – Unlawful Business Practices
(On Behalf of Plaintiff and the Class)**

1
2
3
4 228. Plaintiff re-alleges and incorporates the above allegations as if fully set forth
5 herein.

6 229. Defendant violated Cal. Bus. and Prof. Code § 17200, *et seq.*, by engaging in
7 unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or
8 misleading advertising that constitute acts of “unfair competition” as defined in Cal. Bus. Prof.
9 Code § 17200 with respect to the services provided to the Class.
10

11 230. The acts and omissions identified herein were conceived of, directed from, and
12 emanated from Defendant’s California headquarters and harmed consumers nationwide.

13 231. Defendant engaged in unlawful acts and practices with respect to the services
14 by establishing the sub-standard security practices and procedures described herein; by
15 soliciting and collecting Plaintiff’s and Class Members’ PII with knowledge that the
16 information would not be adequately protected; and by storing Plaintiff’s and Class Members’
17 PII in an unsecure electronic environment in violation of California’s data breach statute, Cal.
18 Civ. Code § 1798.81.5, which requires Defendant to take reasonable methods of safeguarding
19 the PII of Plaintiff and the Class Members.
20

21 232. In addition, Defendant engaged in unlawful acts and practices by failing to
22 disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by
23 Cal. Civ. Code § 1798.82.
24

25 233. Defendant also violated its posted privacy policy, knowingly and willfully or
26 negligently and materially, in violation of Cal. Bus. & Prof. Code § 22576.
27
28

1 234. Defendant also violated Section 5 of the FTC Act by failing to employ
2 reasonable and adequate data security safeguards.

3 235. Defendant further committed unfair acts by failing to employ adequate and
4 reasonable safeguards.

5 236. Defendant's conduct was immoral, unethical, oppressive, unscrupulous, and
6 substantially injurious to Plaintiffs and Class Members. Further, Defendant's conduct narrowly
7 benefitted its own business interests at the expense of Plaintiff's and Class Members'
8 fundamental property and privacy interests protected by the California Constitution and the
9 common law.

10 237. As a direct and proximate result of Defendant's unlawful and unfair practices
11 and acts, Plaintiff and Class Members were injured and lost money or property, including but
12 not limited to: receiving employment positions of a lesser value than the bargains they struck
13 with Defendant, the loss of Plaintiff's and Class Members' legally protected interest in the
14 confidentiality and privacy of their PII, nominal damages, and additional losses as described
15 herein.

16 238. Plaintiff and Class Members have suffered harm in the form of lost property
17 value, specifically the diminution of the value of their private and personally identifiable data.

18 239. Defendant's actions caused damage to and loss of Plaintiff's and Class
19 Members' property right to control the dissemination and use of their personal information and
20 communications.

21 240. Defendant knew or should have known that Defendant's computer systems and
22 data security practices were inadequate to safeguard Plaintiff's and Class Members' PII and
23 that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the
24

1 above-named unlawful and unfair practices and acts were negligent, knowing and willful,
2 and/or wanton and reckless with respect to the rights of Plaintiff and Class Members.

3 241. Plaintiff, on behalf of the Class, seeks relief under Cal. Bus. & Prof. Code §
4 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and Class Members of
5 money or property that Defendant may have acquired by means of Defendant’s unlawful, and
6 unfair business practices, restitutionary disgorgement of all profits accruing to Defendant
7 because of Defendant’s unlawful and unfair business practices, declaratory relief, attorneys’
8 fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable
9 relief.
10

11 **COUNT VI**
12 **Violation of the Michigan Consumer Protection Act**
13 **(On Behalf of Plaintiff and the Michigan Subclass)**

14 242. Plaintiff re-alleges and incorporates the above allegations, as if fully set forth
15 herein, and brings this claim on behalf of herself and the Michigan Subclass (the “Class” for
16 the purposes of this count).

17 243. Plaintiff is authorized to bring this claim under Mich. Comp. Laws § 445.911.

18 244. The Michigan Consumer Protection Act (“MCPA”), Mich. Comp. Laws §
19 445.901, *et seq.*, prohibits “unfair, unconscionable, or deceptive methods, acts, or practices in
20 the conduct of trade or commerce” Mich. Comp. Laws § 445.903(1).
21

22 245. As described in this Complaint, Defendant has engaged in the following unfair,
23 unconscionable, and deceptive trade practices that are made unlawful under the MCPA, Mich.
24 Comp. Laws § 445.903(1):

25 (c) Representing that goods or services have sponsorship, approval, characteristics,
26 ingredients, uses, benefits, or quantities that they do not have or that a person has
27 sponsorship, approval, status, affiliation, or connection that she or she does not have;
28

1 (e) Representing that goods or services are of a particular standard, quality, or grade,
2 or that goods are of a particular style or mode, if they are of another;

3 (s) Failing to reveal a material fact, the omission of which tends to mislead or deceive
4 the consumer, and which fact could not reasonably be known by the consumer; and

5 (cc) Failing to reveal facts that are material to the transaction in light of representations
6 of fact made in a positive manner.

7 246. Defendant's deceptive acts or practices in the conduct of commerce include, but
8 are not limited to:

9 a. Failing to implement and maintain reasonable security and privacy measures to
10 protect Plaintiff's and Class members' PII, which was a direct and proximate
11 cause of the Data Breach;

12 b. Failing to identify foreseeable security and privacy risks, remediate identified
13 security and privacy risks, and adequately improve security and privacy
14 measures following previous cybersecurity incidents in the industry, which were
15 direct and proximate causes of the Data Breach;

16 c. Failing to comply with common law and statutory duties pertaining to the
17 security and privacy of Plaintiff's and Class members' PII, including but not
18 limited to duties imposed by the FTC Act, which were direct and proximate
19 causes of the Data Breach;

20 d. Misrepresenting that it would protect the privacy and confidentiality of
21 Plaintiff's and Class members' PII, including by implementing and maintaining
22 reasonable security measures;

23 e. Misrepresenting that it would comply with common law, statutory, and self-
24 imposed duties pertaining to the security and privacy of Plaintiff's and Class
25 members' PII;
26
27
28

- 1 f. Omitting, suppressing, and concealing the material fact that it did not reasonably
2 or adequately secure Plaintiff's and Class members' PII;
- 3 g. Omitting, suppressing, and concealing the material fact that it did not comply
4 with common law, statutory, and self-imposed duties pertaining to the security
5 and privacy of Plaintiff's and Class members' PII; and
- 6
- 7 h. Failing to promptly and adequately notify Plaintiff and the Class that their PII
8 was accessed by unauthorized persons in the Data Breach.

9 247. Defendant is engaged in, and its acts and omissions affect, trade and commerce.
10 Defendant's relevant acts, practices, and omissions complained of in this action were done in
11 the course of Defendant's business of marketing, offering for sale, and selling goods and
12 services throughout the United States.

13

14 248. Defendant had exclusive knowledge of material information regarding its
15 deficient security policies and practices, and regarding the security of Plaintiff's and Class
16 members' PII. This exclusive knowledge includes, but is not limited to, information that
17 Defendant received through internal and other non-public audits and reviews that concluded
18 that Defendant's security policies were substandard and deficient, and that Plaintiff's and Class
19 members' PII and other Defendant data was vulnerable.

20

21 249. Defendant had exclusive knowledge about the extent of the Data Breach,
22 including during the days, weeks, and months following the Data Breach.

23 250. Defendant also had exclusive knowledge about the length of time that it
24 maintained individuals' PII after they stopped being employed at Defendant that necessitated
25 the transfer of that PII to Defendant.

26

27

28

1 251. Defendant failed to disclose, and actively concealed, the material information it
2 had regarding Defendant's deficient security policies and practices, and regarding the security
3 of the sensitive PII. For example, even though Defendant has long known, through internal
4 audits and otherwise, that its security policies and practices were substandard and deficient,
5 and that Plaintiff's and Class members' PII was vulnerable as a result, Defendant failed to
6 disclose this information to, and actively concealed this information from, Plaintiff, Class
7 members and the public. Defendant also did not disclose, and actively concealed, information
8 regarding the extensive length of time that it maintains former employees' PII and other
9 records. Likewise, during the days and weeks following the Data Breach, Defendant failed to
10 disclose, and actively concealed, information that it had regarding the extent and nature of the
11 Data Breach.
12

13 252. Defendant had a duty to disclose the material information that it had because,
14 *inter alia*, it had exclusive knowledge of the information, it actively concealed the information,
15 and because Defendant was in a fiduciary position by virtue of the fact that Defendant collected
16 and maintained Plaintiff's and Class members' PII.
17

18 253. Defendant's representations and omissions were material because they were
19 likely to deceive reasonable individuals about the adequacy of Defendant's data security and
20 its ability to protect the confidentiality of current and former employees' PII.
21

22 254. Had Defendant disclosed to Plaintiff and the Class that its data systems were not
23 secure and, thus, vulnerable to attack, Defendant would have been unable to continue in
24 business without adopting reasonable data security measures and complying with the law.
25 Instead, Defendant received, maintained, and compiled Plaintiff's and Class members' PII
26
27
28

1 without advising that Defendant's data security practices were insufficient to maintain the
2 safety and confidentiality of their PII.

3 255. Accordingly, Plaintiff and Class members acted reasonably in relying on
4 Defendant's misrepresentations and omissions, the truth of which they could not have
5 discovered.

6 256. Defendant's practices were also contrary to legislatively declared and public
7 policies that seek to protect data and ensure that entities who solicit or are entrusted with
8 personal data utilize appropriate security measures, as reflected in laws, such as the FTC Act.

9 257. The injuries suffered by Plaintiff and the Class greatly outweigh any potential
10 countervailing benefit to consumers or to competition and are not injuries that Plaintiff and the
11 Class should have reasonably avoided.

12 258. The damages, ascertainable losses and injuries, including to their money or
13 property, suffered by Plaintiff and the Class as a direct result of Defendant's deceptive acts
14 and practices as set forth herein include, without limitation: (i) invasion of privacy; (ii) theft of
15 their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with
16 attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the
17 bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences
18 of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii)
19 statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to
20 their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and
21 abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized
22 disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect
23 the PII.
24
25
26
27
28

- 1 iii. requiring Defendant to delete, destroy, and purge the personal
2 identifying information of Plaintiff and Class Members unless
3 Defendant can provide to the Court reasonable justification for the
4 retention and use of such information when weighed against the privacy
5 interests of Plaintiff and Class Members;
6
7 iv. requiring Defendant to implement and maintain a comprehensive
8 Information Security Program designed to protect the confidentiality
9 and integrity of the PII of Plaintiff and Class Members;
10 v. prohibiting Defendant from maintaining the PII of Plaintiff and Class
11 Members on a cloud-based database;
12
13 vi. requiring Defendant to engage independent third-party security
14 auditors/penetration testers as well as internal security personnel to
15 conduct testing, including simulated attacks, penetration tests, and
16 audits on Defendant's systems on a periodic basis, and ordering
17 Defendant to promptly correct any problems or issues detected by such
18 third-party security auditors;
19
20 vii. requiring Defendant to engage independent third-party security
21 auditors and internal personnel to run automated security monitoring;
22
23 viii. requiring Defendant to audit, test, and train their security personnel
24 regarding any new or modified procedures; requiring Defendant to
25 segment data by, among other things, creating firewalls and access
26 controls so that if one area of Defendant's network is compromised,
27 hackers cannot gain access to other portions of Defendant's systems;
28

- 1 ix. requiring Defendant to conduct regular database scanning and securing
2 checks;
- 3 x. requiring Defendant to establish an information security training
4 program that includes at least annual information security training for
5 all employees, with additional training to be provided as appropriate
6 based upon the employees' respective responsibilities with handling
7 personal identifying information, as well as protecting the personal
8 identifying information of Plaintiff and Class Members;
- 9
10 xi. requiring Defendant to routinely and continually conduct internal
11 training and education, and on an annual basis to inform internal
12 security personnel how to identify and contain a breach when it occurs
13 and what to do in response to a breach;
- 14
15 xii. requiring Defendant to implement a system of tests to assess its
16 respective employees' knowledge of the education programs discussed
17 in the preceding subparagraphs, as well as randomly and periodically
18 testing employees compliance with Defendant's policies, programs, and
19 systems for protecting personal identifying information;
- 20
21 xiii. requiring Defendant to implement, maintain, regularly review, and
22 revise as necessary a threat management program designed to
23 appropriately monitor Defendant's information networks for threats,
24 both internal and external, and assess whether monitoring tools are
25 appropriately configured, tested, and updated;
- 26
27
28

1 John J. Nelson (SBN 317598)
2 **MILBERG COLEMAN BRYSON**
3 **PHILLIPS GROSSMAN, LLC**
4 402 W. Broadway, Suite 1760
5 San Diego, CA 92101
6 Telephone: (858) 209-6941
7 Email: jnelson@milberg.com

8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
Counsel for Plaintiff and the Proposed Class

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Deficient Cybersecurity Caused Advantis Global 2022 Data Breach, Class Action Lawsuit Alleges](#)
