

1 John J. Nelson (SBN 317598)
2 **MILBERG COLEMAN BRYSON**
3 **PHILLIPS GROSSMAN, PLLC**
4 280 S. Beverly Drive
5 Beverly Hills, CA 90212
6 Telephone: (858) 209-6941
7 Email: jnelson@milberg.com

8 *Attorney for Plaintiff and the Proposed Class*

9
10 **IN THE UNITED STATES DISTRICT COURT**
11 **CENTRAL DISTRICT OF CALIFORNIA**

12 WILLIAM GLICKMAN, on behalf of
13 himself and all others similarly situated,

14 Plaintiff,

15 v.

16 FIRST AMERICAN FINANCIAL
17 CORPORATION,

18 Defendant.

Case No.: _____

CLASS ACTION COMPLAINT

DEMAND FOR A JURY TRIAL

19 Plaintiff William Glickman (“Plaintiff”) brings this Class Action Complaint
20 (“Complaint”) against First American Financial Corporation (“Defendant”) as an
21 individual and on behalf of all others similarly situated, and alleges, upon personal
22 knowledge as to his own actions and his counsels’ investigation, and upon
23 information and belief as to all other matters, as follows:
24
25
26
27
28

SUMMARY OF ACTION

1
2 1. Plaintiff brings this class action against Defendant for its failure to
3
4 properly secure and safeguard sensitive information of its clients’ customers.

5 2. Defendant is a financial company that provides "comprehensive title
6 insurance protection and professional settlement services."¹
7

8 3. Plaintiff’s and Class Members’ sensitive personal information—which
9 they entrusted to Defendant on the mutual understanding that Defendant would
10 protect it against disclosure—was targeted, compromised and unlawfully accessed
11 due to the Data Breach.
12

13 4. Defendant collected and maintained certain personally identifiable
14 information and protected health information of Plaintiff and the putative Class
15 Members (defined below), who are (or were) customers at Defendant’s clients.
16

17 5. The PII compromised in the Data Breach included Plaintiff’s and Class
18 Members’ full names, dates of birth, and Social Security numbers (“personally
19 identifiable information” or “PII”).
20

21 6. The PII compromised in the Data Breach was exfiltrated by cyber-
22 criminals and remains in the hands of those cyber-criminals who target PII for its
23 value to identity thieves.
24

25
26
27 _____
28 ¹ <https://www.firstam.com/index.html>

1 7. As a result of the Data Breach, Plaintiff and approximately 41,000 Class
2 Members,² suffered concrete injuries in fact including, but not limited to: (i) invasion
3 of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time
4 and opportunity costs associated with attempting to mitigate the actual consequences
5 of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs
6 associated with attempting to mitigate the actual consequences of the Data Breach;
7 (vii) actual misuse of the compromised data consisting of an increase in spam calls,
8 texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the
9 continued and certainly increased risk to their PII, which: (a) remains unencrypted
10 and available for unauthorized third parties to access and abuse; and (b) remains
11 backed up in Defendant's possession and is subject to further unauthorized
12 disclosures so long as Defendant fails to undertake appropriate and adequate
13 measures to protect the PII.

14
15
16
17
18 8. The Data Breach was a direct result of Defendant's failure to implement
19 adequate and reasonable cyber-security procedures and protocols necessary to
20 protect consumers' PII from a foreseeable and preventable cyber-attack.
21
22
23
24
25

26
27 ² <https://apps.web.maine.gov/online/aevier/ME/40/4c15fef7-6abc-409a-8ccd-762c8ea8f76c.shtml>
28

1 9. Moreover, upon information and belief, Defendant was targeted for a
2 cyber-attack due to its status as a financial company that collects and maintains
3 highly valuable PII on its systems.
4

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

14 11. Defendant disregarded the rights of Plaintiff and Class Members by,
15 *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate
16 and reasonable measures to ensure its data systems were protected against
17 unauthorized intrusions; failing to take standard and reasonably available steps to
18 prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt
19 and accurate notice of the Data Breach.
20
21

22 12. Plaintiff's and Class Members' identities are now at risk because of
23 Defendant's negligent conduct because the PII that Defendant collected and
24 maintained has been accessed and acquired by data thieves.
25
26
27
28

1 13. Armed with the PII accessed in the Data Breach, data thieves have
2 already engaged in identity theft and fraud and can in the future commit a variety of
3 crimes including, *e.g.*, opening new financial accounts in Class Members' names,
4 taking out loans in Class Members' names, using Class Members' information to
5 obtain government benefits, filing fraudulent tax returns using Class Members'
6 information, obtaining driver's licenses in Class Members' names but with another
7 person's photograph, and giving false information to police during an arrest.
8

9
10 14. As a result of the Data Breach, Plaintiff and Class Members have been
11 exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and
12 Class Members must now and in the future closely monitor their financial accounts
13 to guard against identity theft.
14

15
16 15. Plaintiff and Class Members may also incur out of pocket costs, *e.g.*,
17 for purchasing credit monitoring services, credit freezes, credit reports, or other
18 protective measures to deter and detect identity theft.
19

20 16. Plaintiff brings this class action lawsuit on behalf all those similarly
21 situated to address Defendant's inadequate safeguarding of Class Members' PII that
22 it collected and maintained, and for failing to provide timely and adequate notice to
23 Plaintiff and other Class Members that their information had been subject to the
24 unauthorized access by an unknown third party and precisely what specific type of
25 information was accessed.
26
27
28

1 17. Through this Complaint, Plaintiff seeks to remedy these harms on
2 behalf of himself and all similarly situated individuals whose PII was accessed
3 during the Data Breach.
4

5 18. Plaintiff and Class Members have a continuing interest in ensuring that
6 their information is and remains safe, and they should be entitled to injunctive and
7 other equitable relief.
8

9 **JURISDICTION AND VENUE**

10 19. This Court has subject matter jurisdiction over this action under the
11 Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative
12 Class Members, the aggregated claims of the individual Class Members exceed the
13 sum or value of \$5,000,000 exclusive of interest and costs, and members of the
14 proposed Class are citizens of states different from Defendant.³
15
16

17 20. This Court has jurisdiction over Defendant through its business
18 operations in this District, the specific nature of which occurs in this District.
19 Defendant's principal place of business is in this District. Defendant intentionally
20 avails itself of the markets within this District to render the exercise of jurisdiction
21 by this Court just and proper.
22
23
24

25 _____
26 ³ According to the breach report submitted to the Office of the Maine Attorney General, 55
27 Maine residents were impacted in the Data Breach. *See*
28 <https://apps.web.maine.gov/online/aevviewer/ME/40/4c15fef7-6abc-409a-8ccd-762c8ea8f76c.shtml>

1 21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1)
2 because Defendant's principal place of business is located in this District and a
3 substantial part of the events and omissions giving rise to this action occurred in this
4 District.
5

6 **PARTIES**
7

8 22. Plaintiff William Glickman is a resident and citizen of Dana Point,
9 California.
10

11 23. Defendant First American Financial Corporation is a corporation
12 organized under the state laws of Delaware with its principal place of business
13 located in Santa Ana, California.
14

15 **FACTUAL ALLEGATIONS**

16 ***Defendant's Business***

17 24. Defendant is a financial company that provides "comprehensive title
18 insurance protection and professional settlement services."⁴
19

20 25. Plaintiff and Class Members are current and former customers of
21 Defendant's clients.
22

23 26. In the course of their relationship, customers of Defendant's clients,
24 including Plaintiff and Class Members, provided Defendant with at least the
25
26

27 ⁴ <https://www.firstam.com/index.html>
28

1 following: names, dates of birth, Social Security numbers, and other sensitive
2 information.

3
4 27. Upon information and belief, in the course of collecting PII from its
5 clients' customers, including Plaintiff, Defendant promised to provide
6 confidentiality and adequate security for the data it collected from customers through
7 its applicable privacy policy and through other disclosures in compliance with
8 statutory privacy requirements.

9
10 28. Indeed, Defendant provides on its website that: "we take all
11 commercially reasonable steps to ensure your personal information is protected in
12 alignment with all applicable laws and regulations, as appropriate to the sensitivity
13 of your personal information."⁵

14
15
16 29. Plaintiff and the Class Members, as customers at Defendant's clients,
17 relied on these promises and on this sophisticated business entity to keep their
18 sensitive PII confidential and securely maintained, to use this information for
19 business purposes only, and to make only authorized disclosures of this information.
20 Consumers, in general, demand security to safeguard their PII, especially when their
21 Social Security numbers and other sensitive PII is involved.
22
23
24
25
26

27 ⁵ <https://www.firstam.com/privacy-policy/index.html>
28

1 ***The Data Breach***

2 30. On or about June 10, 2024, Defendant began sending Plaintiff and other
3 Data Breach victims an untitled letter (the "Notice Letter"), informing them that:

4 **What Happened?**

5 On December 18, 2023, First American Financial Corporation (“First
6 American”) identified unauthorized activity on certain of its information
7 technology systems. Upon detection of the unauthorized activity, First
8 American took steps to contain, assess, and remediate the incident,
9 including isolating its systems from the Internet. First American also
10 launched an investigation with the assistance of leading external
11 cybersecurity experts to determine the impact and scope of the incident,
12 worked with law enforcement, notified certain regulatory authorities, and
13 eradicated the actor from our network.

14 During its investigation, First American learned that certain individuals’
15 personal information may have been accessed without authorization. First
16 American, with the assistance of data review specialists, worked diligently
17 to determine the types of information that may have been subject to
18 unauthorized access and to whom they relate.

19 **What Personal Information Was Involved?**

20 The personal information involved may include your name and any of the
21 following: Date of Birth, Social Security number.⁶

22 31. Omitted from the Notice Letter were the identity of the cybercriminals
23 who perpetrated this Data Breach, the date(s) of the Data Breach, the details of the
24 root cause of the Data Breach, the vulnerabilities exploited, and the remedial
25

26 ⁶ The “Notice Letter”. A sample copy is available at
27 [https://apps.web.maine.gov/online/aeviewer/ME/40/4c15fef7-6abc-409a-8ccd-
28 762c8ea8f76c.shtml](https://apps.web.maine.gov/online/aeviewer/ME/40/4c15fef7-6abc-409a-8ccd-762c8ea8f76c.shtml)

1 measures undertaken to ensure such a breach does not occur again. To date, these
2 omitted details have not been explained or clarified to Plaintiff and Class Members,
3
4 who retain a vested interest in ensuring that their PII remains protected.

5 32. This “disclosure” amounts to no real disclosure at all, as it fails to
6 inform, with any degree of specificity, Plaintiff and Class Members of the Data
7 Breach’s critical facts. Without these details, Plaintiff’s and Class Members’ ability
8 to mitigate the harms resulting from the Data Breach is severely diminished.
9

10 33. Despite Defendant’s intentional opacity about the root cause of this
11 incident, several facts may be gleaned from the Notice Letter, including: a) that this
12 Data Breach was the work of cybercriminals; b) that the cybercriminals first
13 infiltrated Defendant’s networks and systems, and downloaded data from the
14 networks and systems (aka exfiltrated data, or in layperson’s terms “stole” data; and
15
16 c) that once inside Defendant’s networks and systems, the cybercriminals targeted
17 information including Plaintiff’s and Class Members’ Social Security numbers for
18 download and theft.
19
20

21 34. In the context of notice of data breach letters of this type, Defendant’s
22 use of the phrase “may have been subject to unauthorized access” is misleading
23 lawyer language. Companies only send notice letters because data breach
24 notification laws require them to do so. And such letters are only sent to those
25 persons who Defendant itself has a reasonable belief that such personal information
26
27
28

1 was accessed or acquired by an unauthorized individual or entity. Defendant cannot
2 hide behind legalese – by sending a notice of data breach letter to Plaintiff and Class
3
4 Members, it admits that Defendant itself has a reasonable belief that Plaintiff’s and
5 Class Members’ names, dates of birth, and Social Security numbers were accessed
6 or acquired by an unknown actor – aka cybercriminals.
7

8 35. Moreover, in its Notice Letter, Defendant failed to specify whether it
9 undertook any efforts to contact the approximate 41,000 Class Members whose data
10 was accessed and acquired in the Data Breach to inquire whether any of the Class
11 Members suffered misuse of their data, whether Class Members should report their
12 misuse to Defendant, and whether Defendant set up any mechanism for Class
13 Members to report any misuse of their data.
14

15 36. Defendant had obligations created by the FTC Act, Gramm-Leach-
16 Bliley Act, contract, common law, and industry standards to keep Plaintiff’s and
17 Class Members’ PII confidential and to protect it from unauthorized access and
18 disclosure.
19

20 37. Defendant did not use reasonable security procedures and practices
21 appropriate to the nature of the sensitive information they were maintaining for
22 Plaintiff and Class Members, causing the exposure of PII, such as encrypting the
23 information or deleting it when it is no longer needed.
24
25
26
27
28

1 38. The attacker accessed and acquired files containing unencrypted PII of
2 Plaintiff and Class Members. Plaintiff's and Class Members' PII was accessed and
3
4 stolen in the Data Breach.

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

9 ***Data Breaches Are Preventable***

10 40. Defendant did not use reasonable security procedures and practices
11 appropriate to the nature of the sensitive information they were maintaining for
12 Plaintiff and Class Members, causing the exposure of PII, such as encrypting the
13 information or deleting it when it is no longer needed.
14
15

16 41. Defendant could have prevented this Data Breach by, among other
17 things, properly encrypting or otherwise protecting their equipment and computer
18 files containing PII.
19

20 42. As explained by the Federal Bureau of Investigation, “[p]revention is
21 the most effective defense against ransomware and it is critical to take precautions
22 for protection.”⁷
23
24
25
26

27 ⁷ How to Protect Your Networks from RANSOMWARE, at 3, *available at:*
28 <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>

1 43. To prevent and detect cyber-attacks and/or ransomware attacks,
2 Defendant could and should have implemented, as recommended by the United
3 States Government, the following measures:
4

- 5 • Implement an awareness and training program. Because end users are
6 targets, employees and individuals should be aware of the threat of
7 ransomware and how it is delivered.
- 8 • Enable strong spam filters to prevent phishing emails from reaching the
9 end users and authenticate inbound email using technologies like Sender
10 Policy Framework (SPF), Domain Message Authentication Reporting and
11 Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to
12 prevent email spoofing.
- 13 • Scan all incoming and outgoing emails to detect threats and filter
14 executable files from reaching end users.
- 15 • Configure firewalls to block access to known malicious IP addresses.
- 16 • Patch operating systems, software, and firmware on devices. Consider
17 using a centralized patch management system.
- 18 • Set anti-virus and anti-malware programs to conduct regular scans
19 automatically.
- 20 • Manage the use of privileged accounts based on the principle of least
21 privilege: no users should be assigned administrative access unless
22 absolutely needed; and those with a need for administrator accounts should
23 only use them when necessary.
- 24 • Configure access controls—including file, directory, and network share
25 permissions—with least privilege in mind. If a user only needs to read
26 specific files, the user should not have write access to those files,
27 directories, or shares.
- 28 • Disable macro scripts from office files transmitted via email. Consider
using Office Viewer software to open Microsoft Office files transmitted
via email instead of full office suite applications.

- 1 • Implement Software Restriction Policies (SRP) or other controls to prevent
2 programs from executing from common ransomware locations, such as
3 temporary folders supporting popular Internet browsers or
4 compression/decompression programs, including the
AppData/LocalAppData folder.
- 5 • Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- 6 • Use application whitelisting, which only allows systems to execute
7 programs known and permitted by security policy.
- 8 • Execute operating system environments or specific programs in a
9 virtualized environment.
- 10 • Categorize data based on organizational value and implement physical and
11 logical separation of networks and data for different organizational units.⁸

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

15
16 **Secure internet-facing assets**

- 17 - Apply latest security updates
- 18 - Use threat and vulnerability management
- 19 - Perform regular audit; remove privileged credentials;

20 **Thoroughly investigate and remediate alerts**

- 21 - Prioritize and treat commodity malware infections as potential
22 full compromise;

23 **Include IT Pros in security discussions**

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

27 ⁸ *Id.* at 3-4.

1
2 **Build credential hygiene**

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

6 **Apply principle of least-privilege**

- 7 - Monitor for adversarial activities
8 - Hunt for brute force attempts
9 - Monitor for cleanup of Event Logs
- Analyze logon events;

10 **Harden infrastructure**

- 11
12 - Use Windows Defender Firewall
13 - Enable tamper protection
14 - Enable cloud-delivered protection
15 - Turn on attack surface reduction rules and [Antimalware Scan
Interface] for Office [Visual Basic for Applications].⁹

16 45. Given that Defendant was storing the PII of its clients' current and
17 former customers, Defendant could and should have implemented all of the above
18 measures to prevent and detect cyberattacks.

19
20 46. The occurrence of the Data Breach indicates that Defendant failed to
21 adequately implement one or more of the above measures to prevent cyberattacks,
22 resulting in the Data Breach and data thieves acquiring and accessing the PII of more
23 than forty thousand individuals, including that of Plaintiff and Class Members.
24

25
26 _____
27 ⁹ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at*:
28 <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

1 ***Defendant Acquires, Collects, And Stores Its Clients' Customers' PII***

2 47. Defendant acquires, collects, and stores a massive amount of PII on its
3
4 clients' current and former customers.

5 48. As a condition of obtaining services at Defendant's clients, Defendant
6 requires that its clients' customers and other personnel entrust it with highly sensitive
7
8 personal information.

9 49. By obtaining, collecting, and using Plaintiff's and Class Members' PII,
10 Defendant assumed legal and equitable duties and knew or should have known that
11
12 it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

13 50. Plaintiff and the Class Members have taken reasonable steps to
14 maintain the confidentiality of their PII and would not have entrusted it to Defendant
15
16 absent a promise to safeguard that information.

17 51. Upon information and belief, in the course of collecting PII from
18 customers, including Plaintiff, Defendant promised to provide confidentiality and
19
20 adequate security for their data through its applicable privacy policy and through
21 other disclosures in compliance with statutory privacy requirements.

22 52. Indeed, Defendant provides on its website that: "we take all
23
24 commercially reasonable steps to ensure your personal information is protected in
25
26
27
28

1 alignment with all applicable laws and regulations, as appropriate to the sensitivity
2 of your personal information.”¹⁰

3
4 53. Plaintiff and the Class Members relied on Defendant to keep their PII
5 confidential and securely maintained, to use this information for business purposes
6 only, and to make only authorized disclosures of this information.

7
8 ***Defendant Knew, Or Should Have Known, of the Risk Because Financial***
9 ***Companies In Possession Of PII Are Particularly Susceptible To Cyber***
10 ***Attacks***

11 54. Defendant’s data security obligations were particularly important given
12 the substantial increase in cyber-attacks and/or data breaches targeting financial
13 companies that collect and store PII, like Defendant, preceding the date of the
14 breach.

15
16 55. Data breaches, including those perpetrated against financial companies
17 that store PII in their systems, have become widespread.

18
19 56. In the third quarter of the 2023 fiscal year alone, 7333 organizations
20 experienced data breaches, resulting in 66,658,764 individuals’ personal information
21 being compromised.¹¹

22
23 57. In light of recent high profile data breaches at other industry leading
24 companies, including T-Mobile, USA (37 million records, February-March 2023),

25
26
27 ¹⁰ <https://www.firstam.com/privacy-policy/index.html>

28 ¹¹ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>

1 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company
2 (1.4 million records, June 2023), NCB Management Services, Inc. (1 million
3 records, February 2023), Defendant knew or should have known that the PII that
4 they collected and maintained would be targeted by cybercriminals.
5

6 58. Indeed, cyber-attacks, such as the one experienced by Defendant, have
7 become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S.
8 Secret Service have issued a warning to potential targets so they are aware of, and
9 prepared for, a potential attack. As one report explained, smaller entities that store
10 PII are “attractive to ransomware criminals...because they often have lesser IT
11 defenses and a high incentive to regain access to their data quickly.”¹²
12

13
14 59. Additionally, as companies became more dependent on computer
15 systems to run their business,¹³ e.g., working remotely as a result of the Covid-19
16 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is
17 magnified, thereby highlighting the need for adequate administrative, physical, and
18 technical safeguards.¹⁴
19
20
21
22

23 ¹² 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

24
25
26 ¹³ <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

27 ¹⁴ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>
28

1 60. Defendant knew and understood unprotected or exposed PII in the
2 custody of insurance companies, like Defendant, is valuable and highly sought after
3 by nefarious third parties seeking to illegally monetize that PII through unauthorized
4 access.
5

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

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

17 63. The injuries to Plaintiff and Class Members were directly and
18 proximately caused by Defendant's failure to implement or maintain adequate data
19 security measures for the PII of Plaintiff and Class Members.
20

21 64. The ramifications of Defendant's failure to keep secure the PII of
22 Plaintiff and Class Members are long lasting and severe. Once PII is stolen—
23 particularly Social Security numbers—fraudulent use of that information and
24 damage to victims may continue for years.
25
26
27
28

1 65. In the Notice Letter, Defendant makes an offer of 24 months of identity
2 monitoring services. This is wholly inadequate to compensate Plaintiff and Class
3 Members as it fails to provide for the fact victims of data breaches and other
4 unauthorized disclosures commonly face multiple years of ongoing identity theft,
5 financial fraud, and it entirely fails to provide sufficient compensation for the
6 unauthorized release and disclosure of Plaintiff's and Class Members' PII.
7

8
9 66. Defendant's offer of credit and identity monitoring establishes that
10 Plaintiff's and Class Members' sensitive PII was in fact affected, accessed,
11 compromised, and exfiltrated from Defendant's computer systems.
12

13 67. As a financial company in custody of the PII of its clients' customers,
14 Defendant knew, or should have known, the importance of safeguarding PII
15 entrusted to it by Plaintiff and Class Members, and of the foreseeable consequences
16 if its data security systems were breached. This includes the significant costs
17 imposed on Plaintiff and Class Members as a result of a breach. Defendant failed,
18 however, to take adequate cybersecurity measures to prevent the Data Breach.
19
20

21 ***Value Of Personally Identifying Information***

22 68. The Federal Trade Commission ("FTC") defines identity theft as "a
23 fraud committed or attempted using the identifying information of another person
24 without authority."¹⁵ The FTC describes "identifying information" as "any name or
25
26

27 _____
28 ¹⁵ 17 C.F.R. § 248.201 (2013).

1 number that may be used, alone or in conjunction with any other information, to
2 identify a specific person,” including, among other things, “[n]ame, Social Security
3 number, date of birth, official State or government issued driver’s license or
4 identification number, alien registration number, government passport number,
5 employer or taxpayer identification number.”¹⁶
6

7
8 69. The PII of individuals remains of high value to criminals, as evidenced
9 by the prices they will pay through the dark web. Numerous sources cite dark web
10 pricing for stolen identity credentials.¹⁷
11

12 70. For example, Personal Information can be sold at a price ranging from
13 \$40 to \$200.¹⁸ Criminals can also purchase access to entire company data breaches
14 from \$900 to \$4,500.¹⁹
15

16 71. Moreover, Social Security numbers are among the worst kind of PII to
17 have stolen because they may be put to a variety of fraudulent uses and are difficult
18 for an individual to change.
19
20
21
22

23 ¹⁶ *Id.*

24 ¹⁷ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct.
25 16, 2019, available at: [https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-
26 web-how-much-it-costs/](https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/)

27 ¹⁸ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6,
28 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/)

¹⁹ *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 72. According to the Social Security Administration, each time an
2 individual’s Social Security number is compromised, “the potential for a thief to
3 illegitimately gain access to bank accounts, credit cards, driving records, tax and
4 employment histories and other private information increases.”²⁰ Moreover,
5 “[b]ecause many organizations still use SSNs as the primary identifier, exposure to
6 identity theft and fraud remains.”²¹
7
8

9 73. The Social Security Administration stresses that the loss of an
10 individual’s Social Security number, as experienced by Plaintiff and some Class
11 Members, can lead to identity theft and extensive financial fraud:
12

13 A dishonest person who has your Social Security number can use it to
14 get other personal information about you. Identity thieves can use your
15 number and your good credit to apply for more credit in your name.
16 Then, they use the credit cards and don’t pay the bills, it damages your
17 credit. You may not find out that someone is using your number until
18 you’re turned down for credit, or you begin to get calls from unknown
19 creditors demanding payment for items you never bought. Someone
20 illegally using your Social Security number and assuming your identity
21 can cause a lot of problems.²²
22
23

24 ²⁰ See

25 <https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.>

26 ²¹ *Id.*

27 ²² Social Security Administration, *Identity Theft and Your Social Security Number*, available at:
28 <https://www.ssa.gov/pubs/EN-05-10064.pdf>

1 74. In fact, “[a] stolen Social Security number is one of the leading causes
2 of identity theft and can threaten your financial health.”²³ “Someone who has your
3 SSN can use it to impersonate you, obtain credit and open bank accounts, apply for
4 jobs, steal your tax refunds, get medical treatment, and steal your government
5 benefits.”²⁴
6

7
8 75. What’s more, it is no easy task to change or cancel a stolen Social
9 Security number. An individual cannot obtain a new Social Security number without
10 significant paperwork and evidence of actual misuse. In other words, preventive
11 action to defend against the possibility of misuse of a Social Security number is not
12 permitted; an individual must show evidence of actual, ongoing fraud activity to
13 obtain a new number.
14

15
16 76. Even then, a new Social Security number may not be effective.
17 According to Julie Ferguson of the Identity Theft Resource Center, “[t]he credit
18 bureaus and banks are able to link the new number very quickly to the old number,
19 so all of that old bad information is quickly inherited into the new Social Security
20 number.”²⁵
21
22
23

24 ²³ See [https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-](https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/)
25 [number-identity-theft/](https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/)

26 ²⁴ See <https://www.investopedia.com/terms/s/ssn.asp>

27 ²⁵ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR
28 (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft>

1 77. For these reasons, some courts have referred to Social Security numbers
2 as the “gold standard” for identity theft. *Portier v. NEO Tech. Sols.*, No. 3:17-CV-
3 30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) (“Because Social
4 Security numbers are the gold standard for identity theft, their theft is significant . .
5 . . Access to Social Security numbers causes long-lasting jeopardy because the Social
6 Security Administration does not normally replace Social Security numbers.”),
7 report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D.
8 Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc.*, 2021 WL 860584, at
9 *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiff’s Social
10 Security numbers are: arguably “the most dangerous type of personal information in
11 the hands of identity thieves” because it is immutable and can be used to
12 “impersonat[e] [the victim] to get medical services, government benefits, ... tax
13 refunds, [and] employment.” . . . Unlike a credit card number, which can be changed
14 to eliminate the risk of harm following a data breach, “[a] social security number
15 derives its value in that it is immutable,” and when it is stolen it can “forever be
16 wielded to identify [the victim] and target his in fraudulent schemes and identity
17 theft attacks.”)

18 78. Similarly, the California state government warns consumers that:
19 “[o]riginally, your Social Security number (SSN) was a way for the government to
20 track your earnings and pay you retirement benefits. But over the years, it has
21
22
23
24
25
26
27
28

1 become much more than that. It is the key to a lot of your personal information. With
2 your name and SSN, an identity thief could open new credit and bank accounts, rent
3 an apartment, or even get a job.”²⁶
4

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

13 80. This data demands a much higher price on the black market. Martin
14 Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to
15 credit card information, personally identifiable information and Social Security
16 numbers are worth more than 10x on the black market.”²⁷
17
18

19 81. Among other forms of fraud, identity thieves may obtain driver’s
20 licenses, government benefits, medical services, and housing or even give false
21 information to police.
22
23
24

25 ²⁶ See <https://oag.ca.gov/idtheft/facts/your-ssn>

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

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

7
8 [L]aw enforcement officials told us that in some cases, stolen data may
9 be held for up to a year or more before being used to commit identity
10 theft. Further, once stolen data have been sold or posted on the Web,
11 fraudulent use of that information may continue for years. As a result,
12 studies that attempt to measure the harm resulting from data breaches
cannot necessarily rule out all future harm.²⁸

13 83. Plaintiff and Class Members now face years of constant surveillance of
14 their financial and personal records, monitoring, and loss of rights. The Class is
15 incurring and will continue to incur such damages in addition to any fraudulent use
16 of their PII.
17

18 ***Defendant Fails To Comply With FTC Guidelines***

19
20 84. The Federal Trade Commission (“FTC”) has promulgated numerous
21 guides for businesses which highlight the importance of implementing reasonable
22 data security practices. According to the FTC, the need for data security should be
23 factored into all business decision-making.
24

25
26
27 ²⁸ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:
28 <https://www.gao.gov/assets/gao-07-737.pdf>

1 85. In 2016, the FTC updated its publication, Protecting Personal
2 Information: A Guide for Business, which established cyber-security guidelines for
3 businesses. These guidelines note that businesses should protect the personal
4 consumer information that they keep; properly dispose of personal information that
5 is no longer needed; encrypt information stored on computer networks; understand
6 their network's vulnerabilities; and implement policies to correct any security
7 problems.²⁹
8

9
10 86. The guidelines also recommend that businesses use an intrusion
11 detection system to expose a breach as soon as it occurs; monitor all incoming traffic
12 for activity indicating someone is attempting to hack the system; watch for large
13 amounts of data being transmitted from the system; and have a response plan ready
14 in the event of a breach.³⁰
15
16

17 87. The FTC further recommends that companies not maintain PII longer
18 than is needed for authorization of a transaction; limit access to sensitive data;
19 require complex passwords to be used on networks; use industry-tested methods for
20 security; monitor for suspicious activity on the network; and verify that third-party
21 service providers have implemented reasonable security measures.
22
23
24
25

26 ²⁹ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).
27 Available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-
personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)

28 ³⁰ *Id.*

1 88. The FTC has brought enforcement actions against businesses for failing
2 to adequately and reasonably protect consumer data, treating the failure to employ
3 reasonable and appropriate measures to protect against unauthorized access to
4 confidential consumer data as an unfair act or practice prohibited by Section 5 of the
5 Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from
6 these actions further clarify the measures businesses must take to meet their data
7 security obligations.
8

9
10 89. These FTC enforcement actions include actions against financial
11 companies, like Defendant.
12

13 90. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices
14 in or affecting commerce,” including, as interpreted and enforced by the FTC, the
15 unfair act or practice by businesses, such as Defendant, of failing to use reasonable
16 measures to protect PII. The FTC publications and orders described above also form
17 part of the basis of Defendant's duty in this regard.
18

19
20 91. Defendant failed to properly implement basic data security practices.

21 92. Defendant's failure to employ reasonable and appropriate measures to
22 protect against unauthorized access to the PII of its clients' customers or to comply
23 with applicable industry standards constitutes an unfair act or practice prohibited by
24 Section 5 of the FTC Act, 15 U.S.C. § 45.
25
26
27
28

1 93. Upon information and belief, Defendant was at all times fully aware of
2 its obligation to protect the PII of its clients' customers, Defendant was also aware
3 of the significant repercussions that would result from its failure to do so.
4 Accordingly, Defendant's conduct was particularly unreasonable given the nature
5 and amount of PII it obtained and stored and the foreseeable consequences of the
6 immense damages that would result to Plaintiff and the Class.
7

8
9 ***Defendant Failed to Comply with the Gramm-Leach-Bliley Act***

10 94. Defendant is a financial institution, as that term is defined by Section
11 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and
12 thus is subject to the GLBA.
13

14 95. The GLBA defines a financial institution as "any institution the
15 business of which is engaging in financial activities as described in Section 1843(k)
16 of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).
17

18 96. Defendant collects nonpublic personal information, as defined by 15
19 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1).
20 Accordingly, during the relevant time period Defendant were subject to the
21 requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq.*, and is subject to numerous
22 rules and regulations promulgated on the GLBA statutes.
23

24 97. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16
25 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the
26
27
28

1 CFPB became responsible for implementing the Privacy Rule. In December 2011,
2 the CFPB restated the implementing regulations in an interim final rule that
3 established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R.
4 § 1016 (“Regulation P”), with the final version becoming effective on October 28,
5 2014.
6

7
8 98. Accordingly, Defendant's conduct is governed by the Privacy Rule
9 prior to December 30, 2011 and by Regulation P after that date.

10 99. Both the Privacy Rule and Regulation P require financial institutions to
11 provide customers with an initial and annual privacy notice. These privacy notices
12 must be “clear and conspicuous.” 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4
13 and 1016.5. “Clear and conspicuous means that a notice is reasonably
14 understandable and designed to call attention to the nature and significance of the
15 information in the notice.” 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These
16 privacy notices must “accurately reflect[] [the financial institution’s] privacy
17 policies and practices.” 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and
18 1016.5. They must include specified elements, including the categories of nonpublic
19 personal information the financial institution collects and discloses, the categories
20 of third parties to whom the financial institution discloses the information, and the
21 financial institution’s security and confidentiality policies and practices for
22 nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These
23
24
25
26
27
28

1 privacy notices must be provided “so that each consumer can reasonably be expected
2 to receive actual notice.” 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein,
3
4 Defendant violated the Privacy Rule and Regulation P.

5 100. Upon information and belief, Defendant failed to provide annual
6 privacy notices to customers after the customer relationship ended, despite retaining
7 these customers’ PII and storing that PII on Defendant's network systems.
8

9 101. Defendant failed to adequately inform their customers that they were
10 storing and/or sharing, or would store and/or share, the customers’ PII on an insecure
11 platform, accessible to unauthorized parties from the internet, and would do so after
12 the customer relationship ended.
13

14 102. The Safeguards Rule, which implements Section 501(b) of the GLBA,
15 15 U.S.C. § 6801(b), requires financial institutions to protect the security,
16 confidentiality, and integrity of customer information by developing a
17 comprehensive written information security program that contains reasonable
18 administrative, technical, and physical safeguards, including: (1) designating one or
19 more employees to coordinate the information security program; (2) identifying
20 reasonably foreseeable internal and external risks to the security, confidentiality, and
21 integrity of customer information, and assessing the sufficiency of any safeguards in
22 place to control those risks; (3) designing and implementing information safeguards
23 to control the risks identified through risk assessment, and regularly testing or
24
25
26
27
28

1 otherwise monitoring the effectiveness of the safeguards' key controls, systems, and
2 procedures; (4) overseeing service providers and requiring them by contract to
3 protect the security and confidentiality of customer information; and (5) evaluating
4 and adjusting the information security program in light of the results of testing and
5 monitoring, changes to the business operation, and other relevant circumstances. 16
6
7
8 C.F.R. §§ 314.3 and 314.4.

9 103. As alleged herein, Defendant violated the Safeguard Rule.

10 104. Defendant failed to assess reasonably foreseeable risks to the security,
11 confidentiality, and integrity of customer information and failed to monitor the
12 systems of its IT partners or verify the integrity of those systems.
13

14 105. Defendant violated the GLBA and its own policies and procedures by
15 sharing the PII of Plaintiff and Class Members with a non-affiliated third party
16 without providing Plaintiff and Class Members (a) an opt-out notice and (b) a
17 reasonable opportunity to opt out of such disclosure.
18
19

20 ***Defendant Fails To Comply With Industry Standards***

21 106. As noted above, experts studying cyber security routinely identify
22 financial companies in possession of PII as being particularly vulnerable to
23 cyberattacks because of the value of the PII which they collect and maintain.
24

25 107. Several best practices have been identified that, at a minimum, should
26 be implemented by financial companies in possession of PII, like Defendant,
27
28

1 including but not limited to: educating all employees; strong passwords; multi-layer
2 security, including firewalls, anti-virus, and anti-malware software; encryption,
3 making data unreadable without a key; multi-factor authentication; backup data and
4 limiting which employees can access sensitive data. Defendant failed to follow these
5 industry best practices, including a failure to implement multi-factor authentication.
6
7

8 108. Other best cybersecurity practices that are standard for financial
9 companies include installing appropriate malware detection software; monitoring
10 and limiting the network ports; protecting web browsers and email management
11 systems; setting up network systems such as firewalls, switches and routers;
12 monitoring and protection of physical security systems; protection against any
13 possible communication system; training staff regarding critical points. Defendant
14 failed to follow these cybersecurity best practices, including failure to train staff.
15
16

17 109. Defendant failed to meet the minimum standards of any of the
18 following frameworks: the NIST Cybersecurity Framework Version 2.0 (including
19 without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05,
20 PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05,
21 PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the
22 Center for Internet Security's Critical Security Controls (CIS CSC), which are all
23 established standards in reasonable cybersecurity readiness.
24
25
26
27
28

1 110. These foregoing frameworks are existing and applicable industry
2 standards for financial companies, and upon information and belief, Defendant failed
3
4 to comply with at least one—or all—of these accepted standards, thereby opening
5 the door to the threat actor and causing the Data Breach.

6 ***Common Injuries & Damages***
7

8 111. As a result of Defendant's ineffective and inadequate data security
9 practices, the Data Breach, and the foreseeable consequences of PII ending up in the
10 possession of criminals, the risk of identity theft to the Plaintiff and Class Members
11 has materialized and is imminent, and Plaintiff and Class Members have all
12 sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of
13 their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs
14 associated with attempting to mitigate the actual consequences of the Data Breach;
15 (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with
16 attempting to mitigate the actual consequences of the Data Breach; (vii) statutory
17 damages; (viii) nominal damages; and (ix) the continued and certainly increased risk
18 to their PII, which: (a) remains unencrypted and available for unauthorized third
19 parties to access and abuse; and (b) remains backed up in Defendant's possession
20 and is subject to further unauthorized disclosures so long as Defendant fails to
21 undertake appropriate and adequate measures to protect the PII.
22
23
24
25
26
27
28

1 ***Data Breaches Increase Victims' Risk Of Identity Theft***

2 112. The unencrypted PII of Class Members will end up for sale on the dark
3 web as that is the *modus operandi* of hackers.
4

5 113. Unencrypted PII may also fall into the hands of companies that will use
6 the detailed PII for targeted marketing without the approval of Plaintiff and Class
7 Members. Simply put, unauthorized individuals can easily access the PII of Plaintiff
8 and Class Members.
9

10 114. The link between a data breach and the risk of identity theft is simple
11 and well established. Criminals acquire and steal PII to monetize the information.
12 Criminals monetize the data by selling the stolen information on the black market to
13 other criminals who then utilize the information to commit a variety of identity theft
14 related crimes discussed below.
15
16

17 115. Plaintiff's and Class Members' PII is of great value to hackers and
18 cyber criminals, and the data stolen in the Data Breach has been used and will
19 continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and
20 Class Members and to profit off their misfortune.
21

22 116. Due to the risk of one's Social Security number being exposed, state
23 legislatures have passed laws in recognition of the risk: "[t]he social security number
24 can be used as a tool to perpetuate fraud against a person and to acquire sensitive
25 personal, financial, medical, and familial information, the release of which could
26
27
28

1 cause great financial or personal harm to an individual. While the social security
2 number was intended to be used solely for the administration of the federal Social
3 Security System, over time this unique numeric identifier has been used extensively
4 for identity verification purposes[.]”³¹

6 117. Moreover, “SSNs have been central to the American identity
7 infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes
8 have also had SSNs baked into their identification process for years. In fact, SSNs
9 have been the gold standard for identifying and verifying the credit history of
10 prospective customers.”³²

13 118. “Despite the risk of fraud associated with the theft of Social Security
14 numbers, just five of the nation’s largest 25 banks have stopped using the numbers
15 to verify a customer’s identity after the initial account setup[.]”³³ Accordingly, since
16 Social Security numbers are frequently used to verify an individual’s identity after
17 logging onto an account or attempting a transaction, “[h]aving access to your Social
18 Security number may be enough to help a thief steal money from your bank
19 account”³⁴

22
23 ³¹ See N.C. Gen. Stat. § 132-1.10(1).

24 ³² See <https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers>

25 ³³ See <https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/>

26 ³⁴ See <https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>

1 119. One such example of criminals piecing together bits and pieces of
2 compromised PII for profit is the development of “Fullz” packages.³⁵

3
4 120. With “Fullz” packages, cyber-criminals can cross-reference two
5 sources of PII to marry unregulated data available elsewhere to criminally stolen
6 data with an astonishingly complete scope and degree of accuracy in order to
7 assemble complete dossiers on individuals.

8
9 121. The development of “Fullz” packages means here that the stolen PII
10 from the Data Breach can easily be used to link and identify it to Plaintiff’s and Class
11 Members’ phone numbers, email addresses, and other unregulated sources and
12 identifiers. In other words, even if certain information such as emails, phone
13 numbers, or credit card numbers may not be included in the PII that was exfiltrated
14 in the Data Breach, criminals may still easily create a Fullz package and sell it at a
15
16
17
18

19 ³⁵ “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://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance->
[\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/)

1 higher price to unscrupulous operators and criminals (such as illegal and scam
2 telemarketers) over and over.

3
4 122. The existence and prevalence of “Fullz” packages means that the PII
5 stolen from the data breach can easily be linked to the unregulated data (like
6 insurance information) of Plaintiff and the other Class Members.

7
8 123. Thus, even if certain information (such as insurance information) was
9 not stolen in the data breach, criminals can still easily create a comprehensive
10 “Fullz” package.

11
12 124. Then, this comprehensive dossier can be sold—and then resold in
13 perpetuity—to crooked operators and other criminals (like illegal and scam
14 telemarketers).

15
16 ***Loss Of Time To Mitigate Risk Of Identity Theft & Fraud***

17 125. As a result of the recognized risk of identity theft, when a Data Breach
18 occurs, and an individual is notified by a company that their PII was compromised,
19 as in this Data Breach, the reasonable person is expected to take steps and spend
20 time to address the dangerous situation, learn about the breach, and otherwise
21 mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend
22 time taking steps to review accounts or credit reports could expose the individual to
23 greater financial harm – yet, the resource and asset of time has been lost.
24
25
26
27
28

1 126. Thus, due to the actual and imminent risk of identity theft, Defendant,
2 in its Notice Letter instructs Plaintiff and Class Members to take the following
3 measures to protect themselves: “remain vigilant against incidents of identity theft
4 and fraud by reviewing your account statements and monitoring your free credit
5 reports for suspicious activity and to detect errors.”³⁶
6

7
8 127. In addition, Defendant’s Notice letter includes a full three pages
9 devoted to “Steps You Can Take To Protect Your Personal Information” that
10 recommend Plaintiff and Class Members to partake in activities such as enrolling in
11 placing fraud alerts on their accounts, placing security freezes on their accounts, and
12 contacting consumer reporting bureaus.³⁷
13

14 128. Defendant’s extensive suggestion of steps that Plaintiff and Class
15 Members must take in order to protect themselves from identity theft and/or fraud
16 demonstrates the significant time that Plaintiff and Class Members must undertake
17 in response to the Data Breach. Plaintiff’s and Class Members’ time is highly
18 valuable and irreplaceable, and accordingly, Plaintiff and Class Members suffered
19 actual injury and damages in the form of lost time that they spent on mitigation
20 activities in response to the Data Breach and at the direction of Defendant’s Notice
21 Letter.
22
23
24

25
26 _____
27 ³⁶ Notice Letter.

28 ³⁷ *Id.*

1 129. Plaintiff and Class Members have spent, and will spend additional time
2 in the future, on a variety of prudent actions, such as researching and verifying the
3 legitimacy of the Data Breach. Accordingly, the Data Breach has caused Plaintiff
4 and Class Members to suffer actual injury in the form of lost time—which cannot be
5 recaptured—spent on mitigation activities.
6

7
8 130. Plaintiff’s mitigation efforts are consistent with the U.S. Government
9 Accountability Office that released a report in 2007 regarding data breaches (“GAO
10 Report”) in which it noted that victims of identity theft will face “substantial costs
11 and time to repair the damage to their good name and credit record.”³⁸
12

13 131. Plaintiff’s mitigation efforts are also consistent with the steps that FTC
14 recommends that data breach victims take several steps to protect their personal and
15 financial information after a data breach, including: contacting one of the credit
16 bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven
17 years if someone steals their identity), reviewing their credit reports, contacting
18 companies to remove fraudulent charges from their accounts, placing a credit freeze
19 on their credit, and correcting their credit reports.³⁹
20
21

22
23 132. And for those Class Members who experience actual identity theft and
24 fraud, the United States Government Accountability Office released a report in 2007
25

26 ³⁸ See United States Government Accountability Office, GAO-07-737, Personal Information: Data
27 Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full
28 Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

³⁹ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

1 regarding data breaches (“GAO Report”) in which it noted that victims of identity
2 theft will face “substantial costs and time to repair the damage to their good name
3 and credit record.”^[4]

5 ***Diminution of Value of PII***

6 133. PII is a valuable property right.⁴⁰ Its value is axiomatic, considering the
7 value of Big Data in corporate America and the consequences of cyber thefts include
8 heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond
9 doubt that PII has considerable market value.

10
11
12 134. Sensitive PII can sell for as much as \$363 per record according to the
13 Infosec Institute.⁴¹

14
15 135. An active and robust legitimate marketplace for PII also exists. In 2019,
16 the data brokering industry was worth roughly \$200 billion.⁴²

17 136. In fact, the data marketplace is so sophisticated that consumers can
18 actually sell their non-public information directly to a data broker who in turn
19 aggregates the information and provides it to marketers or app developers.^{43,44}

21
22 ⁴⁰ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited;
23 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”).

24 ⁴¹ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable
25 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).

26 ⁴² See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015),
<https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

27 ⁴³ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

28 ⁴⁴ <https://datacoup.com/>

1 137. Consumers who agree to provide their web browsing history to the
2 Nielsen Corporation can receive up to \$50.00 a year.⁴⁵
3

4 138. As a result of the Data Breach, Plaintiff's and Class Members' PII,
5 which has an inherent market value in both legitimate and dark markets, has been
6 damaged and diminished by its compromise and unauthorized release. However, this
7 transfer of value occurred without any consideration paid to Plaintiff or Class
8 Members for their property, resulting in an economic loss. Moreover, the PII is now
9 readily available, and the rarity of the Data has been lost, thereby causing additional
10 loss of value.
11

12
13 139. At all relevant times, Defendant knew, or reasonably should have
14 known, of the importance of safeguarding the PII of Plaintiff and Class Members,
15 and of the foreseeable consequences that would occur if Defendant's data security
16 system was breached, including, specifically, the significant costs that would be
17 imposed on Plaintiff and Class Members as a result of a breach.
18

19
20 140. The fraudulent activity resulting from the Data Breach may not come
21 to light for years.
22

23 141. Plaintiff and Class Members now face years of constant surveillance of
24 their financial and personal records, monitoring, and loss of rights. The Class is
25
26

27 _____
28 ⁴⁵ <https://digi.me/what-is-digime/>

1 incurring and will continue to incur such damages in addition to any fraudulent use
2 of their PII.

3
4 142. Defendant was, or should have been, fully aware of the unique type and
5 the significant volume of data on Defendant's network, amounting to more than forty
6 thousand individuals' detailed personal information and, thus, the significant
7 number of individuals who would be harmed by the exposure of the unencrypted
8 data.
9

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

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

16 144. Given the type of targeted attack in this case, sophisticated criminal
17 activity, and the type of PII involved, there is a strong probability that entire batches
18 of stolen information have been placed, or will be placed, on the black market/dark
19 web for sale and purchase by criminals intending to utilize the PII for identity theft
20 crimes –e.g., opening bank accounts in the victims' names to make purchases or to
21 launder money; file false tax returns; take out loans or lines of credit; or file false
22 unemployment claims.
23
24

25
26 145. Such fraud may go undetected until debt collection calls commence
27 months, or even years, later. An individual may not know that his or her PII was
28

1 used to file for unemployment benefits until law enforcement notifies the
2 individual's employer of the suspected fraud. Fraudulent tax returns are typically
3
4 discovered only when an individual's authentic tax return is rejected.

5 146. Consequently, Plaintiff and Class Members are at an increased risk of
6 fraud and identity theft for many years into the future.

7
8 147. The retail cost of credit monitoring and identity theft monitoring can
9 cost around \$200 a year per Class Member. This is reasonable and necessary cost to
10 monitor to protect Class Members from the risk of identity theft that arose from
11 Defendant's Data Breach.

12
13 ***Loss Of Benefit Of The Bargain***

14 148. Furthermore, Defendant's poor data security practices deprived
15 Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay
16 Defendant's clients for financial services, Plaintiff and other reasonable consumers
17 understood and expected that they were, in part, paying for the product and/or service
18 and necessary data security to protect the PII, when in fact, Defendant did not
19 provide the expected data security. Accordingly, Plaintiff and Class Members
20 received services that were of a lesser value than what they reasonably expected to
21 receive under the bargains they struck with Defendant's clients.
22
23
24
25
26
27
28

1 ***Plaintiff William Glickman’s Experience***

2 149. Upon information and belief, Plaintiff William Glickman has a
3 mortgage through Defendant’s client.
4

5 150. As a condition of obtaining mortgage services from Defendant’s client,
6 he was required to provide his PII to Defendant, including his name, date of birth,
7 Social Security number, and other sensitive information.
8

9 151. Upon information and belief, at the time of the Data Breach, Defendant
10 maintained Plaintiff’s PII in its system.
11

12 152. Plaintiff Glickman is very careful about sharing his sensitive PII.
13 Plaintiff stores any documents containing his PII in a safe and secure location. He
14 has never knowingly transmitted unencrypted sensitive PII over the internet or any
15 other unsecured source. Plaintiff would not have entrusted his PII to Defendant had
16 he known of Defendant’s lax data security policies.
17

18 153. Plaintiff William Glickman received the Notice Letter, by U.S. mail,
19 directly from Defendant, dated June 10, 2024. According to the Notice Letter,
20 Plaintiff’s PII was improperly accessed and obtained by unauthorized third parties,
21 including his name, date of birth, and Social Security number.
22

23 154. As a result of the Data Breach, and at the direction of Defendant’s
24 Notice Letter, which instructs Plaintiff to “remain vigilant against incidents of
25 identity theft and fraud by reviewing your account statements and monitoring your
26
27
28

1 free credit reports for suspicious activity and to detect errors[,]”⁴⁶ Plaintiff made
2 reasonable efforts to mitigate the impact of the Data Breach, including researching
3 and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time
4 dealing with the Data Breach—valuable time Plaintiff otherwise would have spent
5 on other activities, including but not limited to work and/or recreation. This time has
6 been lost forever and cannot be recaptured.
7
8

9 155. Plaintiff suffered actual injury from having his PII compromised as a
10 result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii)
11 theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity
12 costs associated with attempting to mitigate the actual consequences of the Data
13 Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with
14 attempting to mitigate the actual consequences of the Data Breach; (vii) statutory
15 damages; (viii) nominal damages; and (ix) the continued and certainly increased risk
16 to his PII, which: (a) remains unencrypted and available for unauthorized third
17 parties to access and abuse; and (b) remains backed up in Defendant’s possession
18 and is subject to further unauthorized disclosures so long as Defendant fails to
19 undertake appropriate and adequate measures to protect the PII.
20
21
22
23

24 156. Plaintiff additionally suffered actual injury in the form of experiencing
25 an increase in spam calls, texts, and/or emails, which, upon information and belief,
26

27 ⁴⁶ Notice Letter.
28

1 was caused by the Data Breach. This misuse of his PII was caused, upon information
2 and belief, by the fact that cybercriminals are able to easily use the information
3 compromised in the Data Breach to find more information about an individual, such
4 as their phone number or email address, from publicly available sources, including
5 websites that aggregate and associate personal information with the owner of such
6 information. Criminals often target data breach victims with spam emails, calls, and
7 texts to gain access to their devices with phishing attacks or elicit further personal
8 information for use in committing identity theft or fraud.
9
10

11
12 157. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress,
13 which has been compounded by the fact that Defendant has still not fully informed
14 him of key details about the Data Breach's occurrence.
15

16 158. As a result of the Data Breach, Plaintiff anticipates spending
17 considerable time and money on an ongoing basis to try to mitigate and address
18 harms caused by the Data Breach.
19

20 159. As a result of the Data Breach, Plaintiff is at a present risk and will
21 continue to be at increased risk of identity theft and fraud for years to come.
22

23 160. Plaintiff William Glickman has a continuing interest in ensuring that his
24 PII, which, upon information and belief, remains backed up in Defendant's
25 possession, is protected and safeguarded from future breaches.
26
27
28

1 **CLASS ALLEGATIONS**

2 161. Plaintiff brings this nationwide class action on behalf of himself and on
3
4 behalf of all others similarly situated, pursuant to Fed. R. Civ. P. 23(a), 23(b)(1),
5 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5).

6 162. The Classes that Plaintiff seeks to represent is defined as follows:

7
8 **Nationwide Class**

9 All individuals residing in the United States whose PII was accessed
10 and/or acquired by an unauthorized party as a result of the data breach
11 reported by Defendant in June 2024 (the “Class”).

12 **California Subclass**

13 All individuals residing in the State of California whose PII was
14 accessed and/or acquired by an unauthorized party as a result of the data
15 breach reported by Defendant in June 2024 (the “California Subclass”).

16 163. Excluded from the Classes are the following individuals and/or entities:
17 Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors,
18 and any entity in which Defendant have a controlling interest; all individuals who
19 make a timely election to be excluded from this proceeding using the correct protocol
20 for opting out; and all judges assigned to hear any aspect of this litigation, as well as
21 their immediate family members.

22 164. Plaintiff reserves the right to amend the definitions of the Classes or
23 add a Class or Subclass if further information and discovery indicate that the
24 definitions of the Class should be narrowed, expanded, or otherwise modified.
25
26
27
28

1 165. Numerosity: The members of the Class are so numerous that joinder of
2 all members is impracticable, if not completely impossible. According to the breach
3 report submitted to the Office of the Maine Attorney General, at least 41,000 Class
4 Members were impacted in the Data Breach.⁴⁷ The Class is apparently identifiable
5 within Defendant's records, and Defendant has already identified these individuals
6 (as evidenced by sending them breach notification letters).
7
8

9 166. Common questions of law and fact exist as to all members of the Class
10 and predominate over any questions affecting solely individual members of the
11 Class. Among the questions of law and fact common to the Class that predominate
12 over questions which may affect individual Class members, including the following:
13

- 14 a. Whether and to what extent Defendant had a duty to protect the PII of
15 Plaintiff and Class Members;
- 16 b. Whether Defendant had respective duties not to disclose the PII of
17 Plaintiff and Class Members to unauthorized third parties;
- 18 c. Whether Defendant had respective duties not to use the PII of Plaintiff
19 and Class Members for non-business purposes;
- 20 d. Whether Defendant failed to adequately safeguard the PII of Plaintiff
21 and Class Members for non-business purposes;
- 22 d. Whether Defendant failed to adequately safeguard the PII of Plaintiff
23 and Class Members;
- 24
- 25
- 26

27 ⁴⁷ See <https://apps.web.maine.gov/online/aevier/ME/40/4c15fef7-6abc-409a-8ccd-762c8ea8f76c.shtml>

- 1 e. Whether and when Defendant actually learned of the Data Breach;
- 2 f. Whether Defendant adequately, promptly, and accurately informed
- 3 Plaintiff and Class Members that their PII had been compromised;
- 4
- 5 g. Whether Defendant violated the law by failing to promptly notify
- 6 Plaintiff and Class Members that their PII had been compromised;
- 7
- 8 h. Whether Defendant failed to implement and maintain reasonable
- 9 security procedures and practices appropriate to the nature and scope of
- 10 the information compromised in the Data Breach;
- 11
- 12 i. Whether Defendant adequately addressed and fixed the vulnerabilities
- 13 which permitted the Data Breach to occur;
- 14
- 15 j. Whether Plaintiff and Class Members are entitled to actual damages,
- 16 statutory damages, and/or nominal damages as a result of Defendant's
- 17 wrongful conduct;
- 18
- 19 k. Whether Plaintiff and Class Members are entitled to injunctive relief to
- 20 redress the imminent and currently ongoing harm faced as a result of
- 21 the Data Breach.

22 167. Typicality: Plaintiff's claims are typical of those of the other members

23 of the Class because Plaintiff, like every other Class Member, was exposed to

24 virtually identical conduct and now suffers from the same violations of the law as

25 each other member of the Class.

26

27

28

1 168. Policies Generally Applicable to the Class: This class action is also
2 appropriate for certification because Defendant acted or refused to act on grounds
3 generally applicable to the Class, thereby requiring the Court’s imposition of
4 uniform relief to ensure compatible standards of conduct toward the Class Members
5 and making final injunctive relief appropriate with respect to the Class as a whole.
6 Defendant's policies challenged herein apply to and affect Class Members uniformly
7 and Plaintiff’s challenges of these policies hinges on Defendant's conduct with
8 respect to the Class as a whole, not on facts or law applicable only to Plaintiff.
9
10

11 169. Adequacy: Plaintiff will fairly and adequately represent and protect the
12 interests of the Class Members in that he has no disabling conflicts of interest that
13 would be antagonistic to those of the other Class Members. Plaintiff seeks no relief
14 that is antagonistic or adverse to the Class Members and the infringement of the
15 rights and the damages he has suffered are typical of other Class Members. Plaintiff
16 has retained counsel experienced in complex class action and data breach litigation,
17 and Plaintiff intend to prosecute this action vigorously.
18
19
20

21 170. Superiority and Manageability: The class litigation is an appropriate
22 method for fair and efficient adjudication of the claims involved. Class action
23 treatment is superior to all other available methods for the fair and efficient
24 adjudication of the controversy alleged herein; it will permit a large number of Class
25 Members to prosecute their common claims in a single forum simultaneously,
26
27
28

1 efficiently, and without the unnecessary duplication of evidence, effort, and expense
2 that hundreds of individual actions would require. Class action treatment will permit
3 the adjudication of relatively modest claims by certain Class Members, who could
4 not individually afford to litigate a complex claim against large corporations, like
5 Defendant. Further, even for those Class Members who could afford to litigate such
6 a claim, it would still be economically impractical and impose a burden on the courts.
7
8

9 171. The nature of this action and the nature of laws available to Plaintiff
10 and Class Members make the use of the class action device a particularly efficient
11 and appropriate procedure to afford relief to Plaintiff and Class Members for the
12 wrongs alleged because Defendant would necessarily gain an unconscionable
13 advantage since they would be able to exploit and overwhelm the limited resources
14 of each individual Class Member with superior financial and legal resources; the
15 costs of individual suits could unreasonably consume the amounts that would be
16 recovered; proof of a common course of conduct to which Plaintiff was exposed is
17 representative of that experienced by the Class and will establish the right of each
18 Class Member to recover on the cause of action alleged; and individual actions
19 would create a risk of inconsistent results and would be unnecessary and duplicative
20 of this litigation.
21
22
23
24

25 172. The litigation of the claims brought herein is manageable. Defendant's
26 uniform conduct, the consistent provisions of the relevant laws, and the ascertainable
27
28

1 identities of Class Members demonstrates that there would be no significant
2 manageability problems with prosecuting this lawsuit as a class action.

3
4 173. Adequate notice can be given to Class Members directly using
5 information maintained in Defendant's records.

6
7 174. Unless a Class-wide injunction is issued, Defendant may continue in its
8 failure to properly secure the PII of Class Members, Defendant may continue to
9 refuse to provide proper notification to Class Members regarding the Data Breach,
10 and Defendant may continue to act unlawfully as set forth in this Complaint.

11
12 175. Further, Defendant has acted on grounds that apply generally to the
13 Class as a whole, so that class certification, injunctive relief, and corresponding
14 declaratory relief are appropriate on a class- wide basis.

15
16 176. Likewise, particular issues are appropriate for certification because
17 such claims present only particular, common issues, the resolution of which would
18 advance the disposition of this matter and the parties' interests therein. Such
19 particular issues include, but are not limited to:

- 20
21 a. Whether Defendant failed to timely notify the Plaintiff and the class of
22 the Data Breach;
23
24 b. Whether Defendant owed a legal duty to Plaintiff and the Class to
25 exercise due care in collecting, storing, and safeguarding their PII;
26
27
28

- 1 c. Whether Defendant's security measures to protect their data systems
2 were reasonable in light of best practices recommended by data security
3 experts;
4
- 5 d. Whether Defendant's failure to institute adequate protective security
6 measures amounted to negligence;
7
- 8 e. Whether Defendant failed to take commercially reasonable steps to
9 safeguard consumer PII; and Whether adherence to FTC data security
10 recommendations, and measures recommended by data security experts
11 would have reasonably prevented the Data Breach.
12

13 **CAUSES OF ACTION**

14 **COUNT I**
15 **Negligence**

16 **(On Behalf of Plaintiff and the Class)**

17 177. Plaintiff re-alleges and incorporates by reference all preceding
18 allegations, as if fully set forth herein.
19

20 178. Defendant requires its clients' customers, including Plaintiff and Class
21 Members, to submit non-public PII in the ordinary course of providing its services.
22

23 179. Defendant gathered and stored the PII of Plaintiff and Class Members
24 as part of its business of soliciting its services to its clients, which solicitations and
25 services affect commerce.
26
27
28

1 180. Plaintiff and Class Members entrusted Defendant with their PII with
2 the understanding that Defendant would safeguard their information.
3

4 181. Defendant had full knowledge of the sensitivity of the PII and the types
5 of harm that Plaintiff and Class Members could and would suffer if the PII were
6 wrongfully disclosed.
7

8 182. By voluntarily undertaking and assuming the responsibility to collect
9 and store this data, and in fact doing so, and sharing it and using it for commercial
10 gain, Defendant had a duty of care to use reasonable means to secure and safeguard
11 their computer property—and Class Members’ PII held within it—to prevent
12 disclosure of the information, and to safeguard the information from theft.
13 Defendant’s duty included a responsibility to implement processes by which they
14 could detect a breach of its security systems in a reasonably expeditious period of
15 time and to give prompt notice to those affected in the case of a data breach.
16
17

18 183. Defendant had a duty to employ reasonable security measures under
19 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits
20 “unfair . . . practices in or affecting commerce,” including, as interpreted and
21 enforced by the FTC, the unfair practice of failing to use reasonable measures to
22 protect confidential data.
23
24

25 184. Defendant's duty to use reasonable security measures also arose under
26 the GLBA, under which they were required to protect the security, confidentiality,
27
28

1 and integrity of customer information by developing a comprehensive written
2 information security program that contains reasonable administrative, technical, and
3
4 physical safeguards.

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

10 186. Defendant's duty of care to use reasonable security measures arose as a
11 result of the special relationship that existed between Defendant and Plaintiff and
12 Class Members. That special relationship arose because Plaintiff and the Class
13 entrusted Defendant with their confidential PII, a necessary part of being customers
14 at Defendant's clients.
15

16 187. Defendant's duty to use reasonable care in protecting confidential data
17 arose not only as a result of the statutes and regulations described above, but also
18 because Defendant is bound by industry standards to protect confidential PII.
19

20 188. Defendant was subject to an "independent duty," untethered to any
21 contract between Defendant and Plaintiff or the Class.
22

23 189. Defendant also had a duty to exercise appropriate clearinghouse
24 practices to remove former customers' PII it was no longer required to retain
25 pursuant to regulations.
26
27
28

1 190. Moreover, Defendant had a duty to promptly and adequately notify
2 Plaintiff and the Class of the Data Breach.

3
4 191. Defendant had and continues to have a duty to adequately disclose that
5 the PII of Plaintiff and the Class within Defendant's possession might have been
6 compromised, how it was compromised, and precisely the types of data that were
7 compromised and when. Such notice was necessary to allow Plaintiff and the Class
8 to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use
9 of their PII by third parties.
10

11
12 192. Defendant breached its duties, pursuant to the FTC Act, GLBA, and
13 other applicable standards, and thus was negligent, by failing to use reasonable
14 measures to protect Class Members' PII. The specific negligent acts and omissions
15 committed by Defendant include, but are not limited to, the following:
16

- 17 a. Failing to adopt, implement, and maintain adequate security measures
18 to safeguard Class Members' PII;
19
20 b. Failing to adequately monitor the security of their networks and
21 systems;
22
23 c. Allowing unauthorized access to Class Members' PII;
24
25 d. Failing to detect in a timely manner that Class Members' PII had been
26 compromised;
27
28

1 e. Failing to remove former customers' PII it was no longer required to
2 retain pursuant to regulations, and

3
4 f. Failing to timely and adequately notify Class Members about the Data
5 Breach's occurrence and scope, so that they could take appropriate
6 steps to mitigate the potential for identity theft and other damages.
7

8 193. Defendant violated Section 5 of the FTC Act and GLBA by failing to
9 use reasonable measures to protect PII and not complying with applicable industry
10 standards, as described in detail herein. Defendant's conduct was particularly
11 unreasonable given the nature and amount of PII it obtained and stored and the
12 foreseeable consequences of the immense damages that would result to Plaintiff and
13 the Class.
14

15
16 194. Plaintiff and Class Members were within the class of persons the
17 Federal Trade Commission Act and GLBA were intended to protect and the type of
18 harm that resulted from the Data Breach was the type of harm that the statutes were
19 intended to guard against.
20

21 195. Defendant's violation of Section 5 of the FTC Act and GLBA
22 constitutes negligence.
23

24 196. The FTC has pursued enforcement actions against businesses, which,
25 as a result of their failure to employ reasonable data security measures and avoid
26
27
28

1 unfair and deceptive practices, caused the same harm as that suffered by Plaintiff
2 and the Class.

3
4 197. A breach of security, unauthorized access, and resulting injury to
5 Plaintiff and the Class was reasonably foreseeable, particularly in light of
6 Defendant's inadequate security practices.

7
8 198. It was foreseeable that Defendant's failure to use reasonable measures
9 to protect Class Members' PII would result in injury to Class Members. Further, the
10 breach of security was reasonably foreseeable given the known high frequency of
11 cyberattacks and data breaches in the financial industry.

12
13 199. Defendant has full knowledge of the sensitivity of the PII and the types
14 of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully
15 disclosed.

16
17 200. Plaintiff and the Class were the foreseeable and probable victims of any
18 inadequate security practices and procedures. Defendant knew or should have
19 known of the inherent risks in collecting and storing the PII of Plaintiff and the Class,
20 the critical importance of providing adequate security of that PII, and the necessity
21 for encrypting PII stored on Defendant's systems or transmitted through third party
22 systems.
23

24
25 201. It was therefore foreseeable that the failure to adequately safeguard
26 Class Members' PII would result in one or more types of injuries to Class Members.
27
28

1 202. Plaintiff and the Class had no ability to protect their PII that was in, and
2 possibly remains in, Defendant's possession.

3
4 203. Defendant was in a position to protect against the harm suffered by
5 Plaintiff and the Class as a result of the Data Breach.

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

13
14
15
16 205. Defendant has admitted that the PII of Plaintiff and the Class was
17 wrongfully lost and disclosed to unauthorized third persons as a result of the Data
18 Breach.

19
20 206. But for Defendant's wrongful and negligent breach of duties owed to
21 Plaintiff and the Class, the PII of Plaintiff and the Class would not have been
22 compromised.

23
24 207. There is a close causal connection between Defendant's failure to
25 implement security measures to protect the PII of Plaintiff and the Class and the
26 harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of
27

1 Plaintiff and the Class was lost and accessed as the proximate result of Defendant's
2 failure to exercise reasonable care in safeguarding such PII by adopting,
3 implementing, and maintaining appropriate security measures.
4

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

21 209. Additionally, as a direct and proximate result of Defendant's
22 negligence, Plaintiff and the Class have suffered and will suffer the continued risks
23 of exposure of their PII, which remain in Defendant's possession and is subject to
24 further unauthorized disclosures so long as Defendant fails to undertake appropriate
25 and adequate measures to protect the PII in its continued possession.
26
27
28

1 210. Plaintiff and Class Members are entitled to compensatory and
2 consequential damages suffered as a result of the Data Breach.

3
4 211. Plaintiff and Class Members are also entitled to injunctive relief
5 requiring Defendant to (i) strengthen its data security systems and monitoring
6 procedures; (ii) submit to future annual audits of those systems and monitoring
7 procedures; and (iii) continue to provide adequate credit monitoring to all Class
8 Members.
9

10
11 **COUNT II**
12 **Breach Of Third-Party Beneficiary Contract**
(On Behalf of Plaintiff and the Class)

13 212. Plaintiff re-alleges and incorporates by reference all preceding
14 allegations, as if fully set forth herein.
15

16 213. Defendant entered into written contracts with its clients to provide
17 mortgage or other financial services.
18

19 214. In exchange, Defendant agreed, in part, to implement adequate security
20 measures to safeguard the PII of Plaintiff and the Class and to timely and adequately
21 notify them of the Data Breach.
22

23 215. These contracts were made expressly for the benefit of Plaintiff and the
24 Class, as Plaintiff and Class Members were the intended third-party beneficiaries of
25 the contracts entered into between Defendant and its clients. Defendant knew that,
26
27
28

1 if it were to breach these contracts with its clients, the its clients' customers—
2 Plaintiff and Class Members—would be harmed.

3
4 216. Defendant breached the contracts it entered into with its clients by,
5 among other things, failing to (i) use reasonable data security measures, (ii)
6 implement adequate protocols and employee training sufficient to protect Plaintiff's
7 PII from unauthorized disclosure to third parties, and (iii) promptly and adequately
8 notify Plaintiff and Class Members of the Data Breach.
9

10 217. Plaintiff and the Class were harmed by Defendant's breach of its
11 contracts with its clients, as such breach is alleged herein, and are entitled to the
12 losses and damages they have sustained as a direct and proximate result thereof.
13

14 218. Plaintiff and Class Members are also entitled to their costs and
15 attorney's fees incurred in this action.
16

17 **COUNT III**
18 **Unjust Enrichment**
19 **(On Behalf of Plaintiff and the Class)**

20 219. Plaintiff re-alleges and incorporates by reference all preceding
21 allegations, as if fully set forth herein.

22 220. Plaintiff brings this Count in the alternative to the breach of third-party
23 beneficiary contract count above.
24

25 221. Plaintiff and Class Members conferred a monetary benefit on
26 Defendant. Specifically, they provided Defendant with their PII. In exchange,
27
28

1 Plaintiff and Class Members should have had their PII protected with adequate data
2 security.

3
4 222. Defendant knew that Plaintiff and Class Members conferred a benefit
5 upon it and has accepted and retained that benefit by accepting and retaining the PII
6 entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's
7
8 and Class Members' PII for business purposes.

9 223. Defendant failed to secure Plaintiff's and Class Members' PII and,
10 therefore, did not fully compensate Plaintiff or Class Members for the value that
11 their PII provided.

12
13 224. Defendant acquired the PII through inequitable record retention as it
14 failed to investigate and/or disclose the inadequate data security practices previously
15 alleged.

16
17 225. If Plaintiff and Class Members had known that Defendant would not
18 use adequate data security practices, procedures, and protocols to adequately
19 monitor, supervise, and secure their PII, they would have entrusted their PII at
20 Defendant or obtained services at Defendant's clients.

21
22 226. Plaintiff and Class Members have no adequate remedy at law.

23
24 227. Defendant enriched itself by saving the costs it reasonably should have
25 expended on data security measures to secure Plaintiff's and Class Members'
26 Personal Information. Instead of providing a reasonable level of security that would
27
28

1 have prevented the hacking incident, Defendant instead calculated to increase its
2 own profit at the expense of Plaintiff and Class Members by utilizing cheaper,
3 ineffective security measures and diverting those funds to its own profit. Plaintiff
4 and Class Members, on the other hand, suffered as a direct and proximate result of
5 Defendant's decision to prioritize its own profits over the requisite security and the
6 safety of their PII.
7
8

9 228. Under the circumstances, it would be unjust for Defendant to be
10 permitted to retain any of the benefits that Plaintiff and Class Members conferred
11 upon it.
12

13 229. As a direct and proximate result of Defendant's conduct, Plaintiff and
14 Class Members have suffered and will suffer injury, including but not limited to: (i)
15 invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv)
16 lost time and opportunity costs associated with attempting to mitigate the actual
17 consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost
18 opportunity costs associated with attempting to mitigate the actual consequences of
19 the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails;
20 (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly
21 increased risk to their PII, which: (a) remains unencrypted and available for
22 unauthorized third parties to access and abuse; and (b) remains backed up in
23
24
25
26
27
28

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

3
4 230. Plaintiff and Class Members are entitled to full refunds, restitution,
5 and/or damages from Defendant and/or an order proportionally disgorging all
6 profits, benefits, and other compensation obtained by Defendant from its wrongful
7 conduct. This can be accomplished by establishing a constructive trust from which
8 the Plaintiff and Class Members may seek restitution or compensation.
9

10 231. Plaintiff and Class Members may not have an adequate remedy at law
11 against Defendant, and accordingly, they plead this claim for unjust enrichment in
12 addition to, or in the alternative to, other claims pleaded herein.
13

14
15 **COUNT IV**
16 **Violation of California's Unfair Competition Law ("UCL")**
17 **Unlawful Business Practice**
18 **Cal Bus. & Prof. Code § 17200, *et seq.***
19 **(On Behalf of Plaintiff and the Class)**

20 232. Plaintiff re-alleges and incorporates by reference all preceding
21 allegations, as if fully set forth herein.

22 233. Defendant is a "person" defined by Cal. Bus. & Prof. Code § 17201.

23 234. Defendant violated Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL") by
24 engaging in unlawful, unfair, and deceptive business acts and practices.

25 235. Defendant's "unfair" acts and practices include:
26
27
28

- 1 a. by utilizing cheaper, ineffective security measures and diverting those
2 funds to its own profit, instead of providing a reasonable level of
3 security that would have prevented the hacking incident;
- 4
- 5 b. failing to follow industry standard and the applicable, required, and
6 appropriate protocols, policies, and procedures regarding the
7 encryption of data;
- 8
- 9 c. failing to timely and adequately notify Class Members about the Data
10 Breach's occurrence and scope, so that they could take appropriate
11 steps to mitigate the potential for identity theft and other damages;
- 12
- 13 d. Omitting, suppressing, and concealing the material fact that it did not
14 reasonably or adequately secure Plaintiff's and Class Members'
15 personal information; and
- 16
- 17 e. Omitting, suppressing, and concealing the material fact that it did not
18 comply with common law and statutory duties pertaining to the security
19 and privacy of Plaintiff's and Class Members' personal information.
20

21 236. Defendant has engaged in "unlawful" business practices by violating
22 multiple laws, including the FTC Act, 15 U.S.C. § 45, GLBA, and California
23 common law.
24

25 237. Defendant's unlawful, unfair, and deceptive acts and practices include:
26
27
28

- 1 a. Failing to implement and maintain reasonable security and privacy
2 measures to protect Plaintiff's and Class Members' personal
3 information, which was a direct and proximate cause of the Data
4 Breach;
5
6 b. Failing to identify foreseeable security and privacy risks, remediate
7 identified security and privacy risks, which was a direct and proximate
8 cause of the Data Breach;
9
10 c. Failing to comply with common law and statutory duties pertaining to
11 the security and privacy of Plaintiff's and Class Members' personal
12 information, including duties imposed by the FTC Act, 15 U.S.C. § 45
13 and GLBA, which was a direct and proximate cause of the Data Breach;
14
15 d. Misrepresenting that it would protect the privacy and confidentiality of
16 Plaintiff's and Class Members' personal information, including by
17 implementing and maintaining reasonable security measures; and
18
19 e. Misrepresenting that it would comply with common law and statutory
20 duties pertaining to the security and privacy of Plaintiff's and Class
21 Members' personal information, including duties imposed by the FTC
22 Act, 15 U.S.C. § 45 and GLBA.
23
24
25
26
27
28

1 238. Defendant's representations and omissions were material because they
2 were likely to deceive reasonable consumers about the adequacy of Defendant's data
3 security and ability to protect the confidentiality of consumers' personal information.
4

5 239. As a direct and proximate result of Defendant's unfair, unlawful, and
6 fraudulent acts and practices, Plaintiff and Class Members' were injured and lost
7 money or property, which would not have occurred but for the unfair and deceptive
8 acts, practices, and omissions alleged herein, time and expenses related to
9 monitoring their financial accounts for fraudulent activity, an increased, imminent
10 risk of fraud and identity theft, and loss of value of their personal information.
11

12 240. Defendant's violations were, and are, willful, deceptive, unfair, and
13 unconscionable.
14

15 241. Plaintiff and Class Members have lost money and property as a result
16 of Defendant's conduct in violation of the UCL, as stated herein and above.
17

18 242. By deceptively storing, collecting, and disclosing their personal
19 information, Defendant has taken money or property from Plaintiff and Class
20 Members.
21

22 243. Defendant acted intentionally, knowingly, and maliciously to violate
23 California's Unfair Competition Law, and recklessly disregarded Plaintiff's and
24 Class Members' rights.
25
26
27
28

1 244. Plaintiff and Class Members seek all monetary and nonmonetary relief
2 allowed by law, including restitution of all profits stemming from Defendant’s
3 unfair, unlawful, and fraudulent business practices or use of their personal
4 information; declaratory relief; reasonable attorneys’ fees and costs under California
5 Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable
6 relief, including public injunctive relief.
7
8

9 **COUNT V**
10 **Violation of the California Consumer Privacy Act of 2018 (“CCPA”)**
11 **Cal. Civ. Code § 1798, *et seq.***
12 **(On Behalf of Plaintiff and the California Subclass)**

13 245. Plaintiff re-alleges and incorporates by reference all preceding
14 allegations, as if fully set forth herein, and brings this claim on behalf of himself and
15 the California Subclass (the “Class” for the purposes of this count).

16 246. The California Consumer Privacy Act (“CCPA”), Cal. Civ. Code §
17 1798.150(a), creates a private cause of action for violations of the CCPA. Section
18 1798.150(a) specifically provides:
19

20 Any consumer whose nonencrypted and nonredacted personal information, as
21 defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section
22 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or
23 disclosure as a result of the business’s violation of the duty to implement and
24 maintain reasonable security procedures and practices appropriate to the
25 nature of the information to protect the personal information may institute a
civil action for any of the following:

26 (A) To recover damages in an amount not less than one hundred dollars
27 (\$100) and not greater than seven hundred and fifty (\$750) per
28 consumer per incident or actual damages, whichever is greater.

1
2 (B) Injunctive or declaratory relief.

3 (C) Any other relief the court deems proper.

4 247. Defendant is a “business” under § 1798.140(b) in that it is a corporation
5 organized for profit or financial benefit of its shareholders or other owners, with
6 gross revenue in excess of \$25 million.
7

8 248. Plaintiff and Class Members are covered “consumers” under §
9 1798.140(g) in that they are natural persons who are California residents.
10

11 249. The personal information of Plaintiff and the Class Members at issue in
12 this lawsuit constitutes “personal information” under § 1798.150(a) and 1798.81.5,
13 in that the personal information Defendant collects and which was impacted by the
14 cybersecurity attack includes an individual’s first name or first initial and the
15 individual’s last name in combination with one or more of the following data
16 elements, with either the name or the data elements not encrypted or redacted: (i)
17 Social Security number; (ii) Driver’s license number, California identification card
18 number, tax identification number, passport number, military identification number,
19 or other unique identification number issued on a government document commonly
20 used to verify the identity of a specific individual; (iii) account number or credit or
21 debit card number, in combination with any required security code, access code, or
22 password that would permit access to an individual’s financial account; (iv) medical
23 information; (v) health insurance information; (vi) unique biometric data generated
24
25
26
27
28

1 from measurements or technical analysis of human body characteristics, such as a
2 fingerprint, retina, or iris image, used to authenticate a specific individual.

3
4 250. Defendant knew or should have known that its computer systems and
5 data security practices were inadequate to safeguard the Class Members' personal
6 information and that the risk of a data breach or theft was highly likely. Defendant
7 failed to implement and maintain reasonable security procedures and practices
8 appropriate to the nature of the information to protect the personal information of
9 Plaintiff and the Class Members. Specifically, Defendant subjected Plaintiff's and
10 the Class Members' nonencrypted and nonredacted personal information to an
11 unauthorized access and exfiltration, theft, or disclosure as a result of the
12 Defendant's violation of the duty to implement and maintain reasonable security
13 procedures and practices appropriate to the nature of the information, as described
14 herein.
15

16
17
18 251. As a direct and proximate result of Defendant's violation of its duty,
19 the unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and Class
20 Members' personal information included exfiltration, theft, or disclosure through
21 Defendant's servers, systems, and website, and/or the dark web, where hackers
22 further disclosed the personal identifying information alleged herein.
23

24
25 252. As a direct and proximate result of Defendant's acts, Plaintiff and the
26 Class Members were injured and lost money or property, including but not limited
27

1 to the loss of Plaintiff’s and Class Members’ legally protected interest in the
2 confidentiality and privacy of their personal information, stress, fear, and anxiety,
3
4 nominal damages, and additional losses described above.

5 253. Section 1798.150(b) specifically provides that “[n]o [prefiling] notice
6 shall be required prior to an individual consumer initiating an action solely for actual
7
8 pecuniary damages.”

9 254. On June 20, 2024, Plaintiff’s counsel sent a CCPA notice letter to
10 Defendant’s registered service agents via certified mail. If Defendant does not cure
11
12 the effects of the Data Breach, which would require retrieving the PII and securing
13 the PII from continuing and future use, within 30 days of delivery of such CCPA
14 notice letter (which Plaintiff believes any such cure is not possible under these facts
15
16 and circumstances), Plaintiff shall seek actual damages and statutory damages of no
17 less than \$100 and up to \$750 per customer record subject to the Data Breach on
18 behalf of the California Subclass as authorized by the CCPA.

19
20 255. Accordingly, Plaintiff and the Class Members by way of this complaint
21 seek actual pecuniary damages suffered as a result of Defendant’s violations
22
23 described herein.

24 **PRAYER FOR RELIEF**

25 **WHEREFORE**, Plaintiff, on behalf of himself and Class Members, requests
26
27 judgment against Defendant and that the Court grants the following:
28

- 1 A. For an Order certifying the Class, and appointing Plaintiff and his
2 Counsel to represent the Class;
3
- 4 B. For equitable relief enjoining Defendant from engaging in the
5 wrongful conduct complained of herein pertaining to the misuse
6 and/or disclosure of the PII of Plaintiff and Class Members;
7
- 8 C. For injunctive relief requested by Plaintiff, including but not limited
9 to, injunctive and other equitable relief as is necessary to protect the
10 interests of Plaintiff and Class Members, including but not limited to
11 an order:
12
- 13 i. prohibiting Defendant from engaging in the wrongful and unlawful
14 acts described herein;
15
- 16 ii. requiring Defendant to protect, including through encryption, all
17 data collected through the course of its business in accordance with
18 all applicable regulations, industry standards, and federal, state or
19 local laws;
20
- 21 iii. requiring Defendant to delete, destroy, and purge the personal
22 identifying information of Plaintiff and Class Members unless
23 Defendant can provide to the Court reasonable justification for the
24 retention and use of such information when weighed against the
25 privacy interests of Plaintiff and Class Members;
26
27
28

- 1 iv. requiring Defendant to provide out-of-pocket expenses associated
2 with the prevention, detection, and recovery from identity theft, tax
3 fraud, and/or unauthorized use of their PII for Plaintiff's and Class
4 Members' respective lifetimes;
5
6 v. requiring Defendant to implement and maintain a comprehensive
7 Information Security Program designed to protect the
8 confidentiality and integrity of the PII of Plaintiff and Class
9 Members;
10
11 vi. prohibiting Defendant from maintaining the PII of Plaintiff and
12 Class Members on a cloud-based database;
13
14 vii. requiring Defendant to engage independent third-party security
15 auditors/penetration testers as well as internal security personnel to
16 conduct testing, including simulated attacks, penetration tests, and
17 audits on Defendant's systems on a periodic basis, and ordering
18 Defendant to promptly correct any problems or issues detected by
19 such third-party security auditors;
20
21 viii. requiring Defendant to engage independent third-party security
22 auditors and internal personnel to run automated security
23 monitoring;
24
25
26
27
28

- 1 ix. requiring Defendant to audit, test, and train its security personnel
2 regarding any new or modified procedures;
3
4 x. requiring Defendant to segment data by, among other things,
5 creating firewalls and controls so that if one area of Defendant's
6 network is compromised, hackers cannot gain access to portions of
7 Defendant's systems;
8
9 xi. requiring Defendant to conduct regular database scanning and
10 securing checks;
11
12 xii. requiring Defendant to establish an information security training
13 program that includes at least annual information security training
14 for all employees, with additional training to be provided as
15 appropriate based upon the employees' respective responsibilities
16 with handling personal identifying information, as well as
17 protecting the personal identifying information of Plaintiff and
18 Class Members;
19
20 xiii. requiring Defendant to routinely and continually conduct internal
21 training and education, and on an annual basis to inform internal
22 security personnel how to identify and contain a breach when it
23 occurs and what to do in response to a breach;
24
25
26
27
28

1 xiv. requiring Defendant to implement a system of tests to assess its
2 respective employees' knowledge of the education programs
3 discussed in the preceding subparagraphs, as well as randomly and
4 periodically testing employees' compliance with Defendant's
5 policies, programs, and systems for protecting personal identifying
6 information;
7

8 xv. requiring Defendant to implement, maintain, regularly review, and
9 revise as necessary a threat management program designed to
10 appropriately monitor Defendant's information networks for
11 threats, both internal and external, and assess whether monitoring
12 tools are appropriately configured, tested, and updated;
13

14 xvi. requiring Defendant to meaningfully educate all Class Members
15 about the threats that they face as a result of the loss of their
16 confidential personal identifying information to third parties, as
17 well as the steps affected individuals must take to protect himself;
18

19 xvii. requiring Defendant to implement logging and monitoring
20 programs sufficient to track traffic to and from Defendant's
21 servers; and
22

23 xviii. for a period of 10 years, appointing a qualified and independent
24 third party assessor to conduct a SOC 2 Type 2 attestation on an
25
26
27
28

1 annual basis to evaluate Defendant's compliance with the terms of
2 the Court's final judgment, to provide such report to the Court and
3 to counsel for the class, and to report any deficiencies with
4 compliance of the Court's final judgment;
5

6 D. For an award of damages, including actual, nominal, statutory,
7 consequential, and punitive damages, as allowed by law in an amount
8 to be determined;
9

10 E. For an award of attorneys' fees, costs, and litigation expenses, as
11 allowed by law;
12

13 F. For prejudgment interest on all amounts awarded; and
14

15 G. Such other and further relief as this Court may deem just and proper.
16

JURY TRIAL DEMANDED

17 Plaintiff hereby demands a trial by jury on all claims so triable.
18

19 Dated: June 21, 2024

Respectfully Submitted,

20 By: /s/ John J. Nelson

21 John J. Nelson (SBN 317598)

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

22 280 S. Beverly Drive

23 Beverly Hills, CA 90212

24 Telephone: (858) 209-6941

25 Email: jnelson@milberg.com

26 *Attorney for Plaintiff and*
27 *the Proposed Class*
28