

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

8 Jeff Ostrow*
9 **KOPELOWITZ OSTROW P.A.**
10 1 West Las Olas Blvd., Ste. 500
11 Fort Lauderdale, FL 33301
12 Tele: 954-332-4200
13 ostrow@kolawyers.com

14 *Attorneys for Plaintiff and*
15 *The Proposed Class*

16 **Pro Hac Vice application forthcoming*

17 **IN THE UNITED STATES DISTRICT COURT**
18 **NORTHERN DISTRICT OF CALIFORNIA**

19 TYRONE HAMMONDS, on behalf of himself
20 and all others similarly situated,

21 Plaintiff,

22 v.

23 ROBINHOOD MARKETS, INC.,

24 Defendant.

Case No.: _____

CLASS ACTION COMPLAINT
DEMAND FOR A JURY TRIAL

25 Plaintiff Tyrone Hammonds (“Plaintiff”) brings this Class Action Complaint
26 (“Complaint”) against Robinhood Markets, Inc. (“Defendant”) as an individual and on behalf of all
27 others similarly situated, and alleges, upon personal knowledge as to his own actions and his
28 counsels’ investigation, and upon information and belief as to all other matters, as follows:

SUMMARY OF ACTION

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

4 2. Defendant is a financial services company that offers stock trading and investment
5 services to its customers.

6
7 3. Plaintiff's and Class Members' sensitive personal information—which they
8 entrusted to Defendant on the mutual understanding that Defendant would protect it against
9 disclosure—was targeted, compromised and unlawfully accessed due to the Data Breach.

10 4. Defendant collected and maintained certain personally identifiable information of
11 Plaintiff and the putative Class Members (defined below), who are (or were) customers at
12 Defendant.

13
14 5. The PII compromised in the Data Breach included Plaintiff's and Class Members'
15 personally identifiable information ("PII"), including, upon information and belief, their Social
16 Security numbers.

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

19
20 7. As a result of the Data Breach, Plaintiff and Class Members suffered concrete
21 injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost
22 or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to
23 mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost
24 opportunity costs associated with attempting to mitigate the actual consequences of the Data
25 Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their PII,
26 which: (a) remains unencrypted and available for unauthorized third parties to access and abuse;

1 and (b) remains backed up in Defendant's possession and is subject to further unauthorized
2 disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect
3 the PII.

4 8. The Data Breach was a direct result of Defendant's failure to implement adequate
5 and reasonable cyber-security procedures and protocols necessary to protect consumers' PII from
6 a foreseeable and preventable cyber-attack.

7
8 9. Moreover, upon information and belief, Defendant was targeted for a cyber-attack
9 due to its status as a financial services company that collects and maintains highly valuable PII on
10 its systems.

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

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

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

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

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

11 15. Plaintiff and Class Members may also incur out of pocket costs, *e.g.*, for purchasing
12 credit monitoring services, credit freezes, credit reports, or other protective measures to deter and
13 detect identity theft.
14

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

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

23 18. Plaintiff and Class Members have a continuing interest in ensuring that their
24 information is and remains safe, and they should be entitled to injunctive and other equitable relief.
25
26
27
28

1 **JURISDICTION AND VENUE**

2 19. This Court has subject matter jurisdiction over this action under the Class Action
3 Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the
4 aggregated claims of the individual Class Members exceed the sum or value of \$5,000,000
5 exclusive of interest and costs, and members of the proposed Class are citizens of states different
6 from Defendant.
7

8 20. This Court has jurisdiction over Defendant through its business operations in this
9 District, the specific nature of which occurs in this District. Defendant’s principal place of business
10 is in this District. Defendant intentionally avails itself of the markets within this District to render
11 the exercise of jurisdiction by this Court just and proper.
12

13 21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because
14 Defendant’s principal place of business is located in this District and a substantial part of the events
15 and omissions giving rise to this action occurred in this District.
16

17 **PARTIES**

18 22. Plaintiff Tyrone Hammonds is a resident and citizen of Elk Grove, California.

19 23. Defendant Robinhood Markets, Inc. is a company with its principal place of
20 business located in Menlo Park, California.

21 **FACTUAL ALLEGATIONS**

22 ***Defendant's Business***

23 24. Defendant is a financial services company that offers stock trading and investment
24 services to its customers.

25 25. Plaintiff and Class Members are current and former customers at Defendant.
26
27
28

1 26. In the course of their relationship, customers, including Plaintiff and Class
2 Members, provided Defendant with their sensitive PII.

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

8 28. Indeed, Defendant provides on its website that: “At Robinhood, we take privacy
9 and security seriously.”¹

10 29. Plaintiff and the Class Members, as customers of Defendant, relied on these
11 promises and on this sophisticated business entity to keep their sensitive PII confidential and
12 securely maintained, to use this information for business purposes only, and to make only
13 authorized disclosures of this information. Consumers, in general, demand security to safeguard
14 their PII.
15

16 ***The Data Breach***

17 30. The BASHE ransomware gang (formerly known as APT73) claims to have
18 conducted a Data Breach on Defendant’s systems, resulting in the acquisition of millions of
19 records.² BASHE demanded a ransom from Defendant in exchange for a promise to delete the
20 exfiltrated data and demanded that Defendant pay the ransom by October 17, 2024. When
21 Defendant failed to pay by the deadline, BASHE began making the exfiltrated data set available
22 for download on the dark web.
23
24
25

26 ¹ <https://robinhood.com/us/en/support/articles/privacy-policy/>

27 ² <https://rakeshkrish.medium.com/apt73-eraleig-news-unveiling-new-ransomware-group-55aec3e873ff>
28

1 31. Upon information and belief, Plaintiff's and Class Members' PII was targeted,
2 accessed, and acquired in the Data Breach.

3 32. Defendant had obligations created by the FTC Act, Gramm-Leach-Bliley Act,
4 contract, common law, and industry standards to keep Plaintiff's and Class Members' PII
5 confidential and to protect it from unauthorized access and disclosure.
6

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

11 34. The attacker accessed and acquired files containing unencrypted PII of Plaintiff and
12 Class Members. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

13 35. Plaintiff further believes that his PII and that of Class Members was subsequently
14 sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals
15 that commit cyber-attacks of this type.
16

17 ***Data Breaches Are Preventable***

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

23 37. Defendant could have prevented this Data Breach by, among other things, properly
24 encrypting or otherwise protecting their equipment and computer files containing PII.
25
26
27
28

1 38. A ransomware attack is a type of cyberattack that is frequently used to target
2 healthcare providers due to the sensitive patient data they maintain.³ In a ransomware attack the
3 attackers use software to encrypt data on a compromised network, rendering it unusable and
4 demanding payment to restore control over the network.⁴

5
6 39. Companies should treat ransomware attacks as any other data breach incident
7 because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data
8 in cybercriminal forums and dark web marketplaces for additional revenue."⁵ As cybersecurity
9 expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be
10 evidence of its absence [...] the initial assumption should be that data may have been exfiltrated."

11 40. An increasingly prevalent form of ransomware attack is the
12 "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data
13 contained within.⁶ In 2020, over 50% of ransomware attackers exfiltrated data from a network
14 before encrypting it.⁷ Once the data is exfiltrated from a network, its confidential nature is
15 destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a
16 second/future extortion attempt."⁸ And even where companies pay for the return of data attackers

17
18
19 ³ *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at
20 <https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/>

21 ⁴ *Ransomware FAQs*, available at <https://www.cisa.gov/stopransomware/ransomware-faqs>

22 ⁵ *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at
23 <https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends>

24 ⁶ *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at
25 <https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/>

26 ⁷ 2020 Ransomware Marketplace Report, available at <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report>

27 ⁸ *Id.*

1 often leak or sell the data regardless because there is no way to verify copies of the data are
2 destroyed.⁹

3 41. As explained by the Federal Bureau of Investigation, “[p]revention is the most
4 effective defense against ransomware and it is critical to take precautions for protection.”¹⁰

5 42. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could
6 and should have implemented, as recommended by the United States Government, the following
7 measures:
8

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

26 ⁹ *Id.*

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

15 43. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and
16 should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team,
17 the following measures:

18 **Secure internet-facing assets**

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

22 **Thoroughly investigate and remediate alerts**

- 23 - Prioritize and treat commodity malware infections as potential full
24 compromise;

25 **Include IT Pros in security discussions**

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

¹¹ *Id.* at 3-4.

1 **Build credential hygiene**

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

4 **Apply principle of least-privilege**

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

8 **Harden infrastructure**

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

14 44. Given that Defendant was storing the PII of its current and former customers,
15 Defendant could and should have implemented all of the above measures to prevent and detect
16 cyberattacks.

17 45. The occurrence of the Data Breach indicates that Defendant failed to adequately
18 implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach
19 and data thieves acquiring and accessing the PII of, upon information and belief, hundreds of
20 thousands of individuals, including that of Plaintiff and Class Members.

21 ***Defendant Acquires, Collects, And Stores Its Customers' PII***

22 46. Defendant acquires, collects, and stores a massive amount of PII on its current and
23 former customers.

24
25
26

¹² See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at:
27 [https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-
28 preventable-disaster/](https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/)

1 47. As a condition of obtaining services at Defendant, Defendant requires that
2 customers and other personnel entrust it with highly sensitive personal information.

3 48. By obtaining, collecting, and using Plaintiff's and Class Members' PII, Defendant
4 assumed legal and equitable duties and knew or should have known that it was responsible for
5 protecting Plaintiff's and Class Members' PII from disclosure.
6

7 49. Plaintiff and the Class Members have taken reasonable steps to maintain the
8 confidentiality of their PII and would not have entrusted it to Defendant absent a promise to
9 safeguard that information.

10 50. Upon information and belief, in the course of collecting PII from customers,
11 including Plaintiff, Defendant promised to provide confidentiality and adequate security for their
12 data through its applicable privacy policy and through other disclosures in compliance with
13 statutory privacy requirements.
14

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

18 ***Defendant Knew, Or Should Have Known, of the Risk Because Financial Services***
19 ***Companies In Possession Of PII Are Particularly Susceptible To Cyber Attacks***

20 52. Defendant's data security obligations were particularly important given the
21 substantial increase in cyber-attacks and/or data breaches targeting financial services companies
22 that collect and store PII, like Defendant, preceding the date of the breach.

23 53. Data breaches, including those perpetrated against financial services companies
24 that store PII in their systems, have become widespread.
25

26 54. In 2023, an all-time high for data compromises occurred, with 3,205 compromises
27 affecting 353,027,892 total victims. Of the 3,205 recorded data compromises, 809 of them, or
28

1 25.2% were in the medical or healthcare industry. The estimated number of organizations
2 impacted by data compromises has increased by +2,600 percentage points since 2018, and the
3 estimated number of victims has increased by +1400 percentage points. The 2023 compromises
4 represent a 78 percentage point increase over the previous year and a 72 percentage point hike
5 from the previous all-time high number of compromises (1,860) set in 2021.
6

7 55. In light of recent high profile data breaches at other industry leading companies,
8 including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million
9 records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB
10 Management Services, Inc. (1 million records, February 2023), Defendant knew or should have
11 known that the PII that they collected and maintained would be targeted by cybercriminals.
12

13 56. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so
14 notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a
15 warning to potential targets so they are aware of, and prepared for, a potential attack. As one report
16 explained, smaller entities that store PII are “attractive to ransomware criminals...because they
17 often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹³
18

19 57. Additionally, as companies became more dependent on computer systems to run
20 their business,¹⁴ e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of
21
22
23

24
25 ¹³ 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
26 [ion](https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection)

27 ¹⁴<https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>
28

1 Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need
2 for adequate administrative, physical, and technical safeguards.¹⁵

3 58. Defendant knew and understood unprotected or exposed PII in the custody of
4 insurance companies, like Defendant, is valuable and highly sought after by nefarious third parties
5 seeking to illegally monetize that PII through unauthorized access.
6

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

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

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

19 62. The ramifications of Defendant’s failure to keep secure the PII of Plaintiff and Class
20 Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and
21 damage to victims may continue for years.
22

23 63. As a financial services company in custody of the PII of its customers, Defendant
24 knew, or should have known, the importance of safeguarding PII entrusted to it by Plaintiff and
25 Class Members, and of the foreseeable consequences if its data security systems were breached.
26

27 ¹⁵ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>
28

1 This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach.
2 Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

3 ***Value Of Personally Identifying Information***

4 64. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud
5 committed or attempted using the identifying information of another person without authority.”¹⁶
6 The FTC describes “identifying information” as “any name or number that may be used, alone or
7 in conjunction with any other information, to identify a specific person,” including, among other
8 things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s
9 license or identification number, alien registration number, government passport number,
10 employer or taxpayer identification number.”¹⁷

11
12 65. The PII of individuals remains of high value to criminals, as evidenced by the prices
13 they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity
14 credentials.¹⁸

15
16 66. For example, Personal Information can be sold at a price ranging from \$40 to
17 \$200.¹⁹ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²⁰

18 67. Of course, a stolen Social Security number – which, upon information and belief,
19 were compromised for some Class Members in the Data Breach – can be used to wreak untold
20 havoc upon a victim’s personal and financial life. The popular person privacy and credit
21

22 ¹⁶ 17 C.F.R. § 248.201 (2013).

23 ¹⁷ *Id.*

24 ¹⁸ *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-web-how-much-it-costs/>

26 ¹⁹ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6,
27 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

28 ²⁰ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>

1 monitoring service LifeLock by Norton notes “Five Malicious Ways a Thief Can Use Your Social
2 Security Number,” including 1) Financial Identity Theft that includes “false applications for loans,
3 credit cards or bank accounts in your name or withdraw money from your accounts, and which
4 can encompass credit card fraud, bank fraud, computer fraud, wire fraud, mail fraud and
5 employment fraud; 2) Government Identity Theft, including tax refund fraud; 3) Criminal Identity
6 Theft, which involves using someone’s stolen Social Security number as a “get out of jail free
7 card;” 4) Medical Identity Theft, and 5) Utility Fraud.

9 68. It is little wonder that courts have dubbed a stolen Social Security number as the
10 “gold standard” for identity theft and fraud. Social Security numbers are among the worst kind of
11 PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an
12 individual to change.

14 69. According to the Social Security Administration, each time an individual’s Social
15 Security number is compromised, “the potential for a thief to illegitimately gain access to bank
16 accounts, credit cards, driving records, tax and employment histories and other private information
17 increases.”²¹ Moreover, “[b]ecause many organizations still use SSNs as the primary identifier,
18 exposure to identity theft and fraud remains.”²²

20 70. The Social Security Administration stresses that the loss of an individual’s Social
21 Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft
22 and extensive financial fraud:

23 A dishonest person who has your Social Security number can use it to get other
24 personal information about you. Identity thieves can use your number and your

25 ²¹ See

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

27 ²² *Id.*

1 good credit to apply for more credit in your name. Then, they use the credit cards
2 and don't pay the bills, it damages your credit. You may not find out that someone
3 is using your number until you're turned down for credit, or you begin to get calls
4 from unknown creditors demanding payment for items you never bought. Someone
5 illegally using your Social Security number and assuming your identity can cause
6 a lot of problems.²³

7 71. In fact, "[a] stolen Social Security number is one of the leading causes of identity
8 theft and can threaten your financial health."²⁴ "Someone who has your SSN can use it to
9 impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get
10 medical treatment, and steal your government benefits."²⁵

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

16 73. Even then, a new Social Security number may not be effective. According to Julie
17 Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link
18 the new number very quickly to the old number, so all of that old bad information is quickly
19 inherited into the new Social Security number."²⁶

20
21
22
23 ²³ Social Security Administration, *Identity Theft and Your Social Security Number*, available at:
<https://www.ssa.gov/pubs/EN-05-10064.pdf>

24 ²⁴ 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 ²⁵ See <https://www.investopedia.com/terms/s/ssn.asp>

27 ²⁶ 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-](http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft)
[hackers-has-millionsworrying-about-identity-theft](http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft)

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

17 75. Similarly, the California state government warns consumers that: “[o]riginally,
18 your Social Security number (SSN) was a way for the government to track your earnings and pay
19 you retirement benefits. But over the years, it has become much more than that. It is the key to a
20 lot of your personal information. With your name and SSN, an identity thief could open new credit
21 and bank accounts, rent an apartment, or even get a job.”²⁷

23 76. Based on the foregoing, the information compromised in the Data Breach is
24 significantly more valuable than the loss of, for example, credit card information in a retailer data
25 breach because, there, victims can cancel or close credit and debit card accounts. The information
26

27 ²⁷ *See* <https://oag.ca.gov/idtheft/facts/your-ssn>
28

1 compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to
2 change.

3 77. This data demands a much higher price on the black market. Martin Walter, senior
4 director at cybersecurity firm RedSeal, explained, “Compared to credit card information,
5 personally identifiable information and Social Security numbers are worth more than 10x on the
6 black market.”²⁸

7
8 78. Among other forms of fraud, identity thieves may obtain driver’s licenses,
9 government benefits, medical services, and housing or even give false information to police.

10 79. The fraudulent activity resulting from the Data Breach may not come to light for
11 years. There may be a time lag between when harm occurs versus when it is discovered, and also
12 between when PII is stolen and when it is used. According to the U.S. Government Accountability
13 Office (“GAO”), which conducted a study regarding data breaches:
14

15 [L]aw enforcement officials told us that in some cases, stolen data may be held for
16 up to a year or more before being used to commit identity theft. Further, once stolen
17 data have been sold or posted on the Web, fraudulent use of that information may
18 continue for years. As a result, studies that attempt to measure the harm resulting
19 from data breaches cannot necessarily rule out all future harm.²⁹

20 80. Plaintiff and Class Members now face years of constant surveillance of their
21 financial and personal records, monitoring, and loss of rights. The Class is incurring and will
22 continue to incur such damages in addition to any fraudulent use of their PII.
23

24
25 ²⁸ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*
26 *Numbers*, IT World, (Feb. 6, 2015), available at:
<https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>

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

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

2 81. The Federal Trade Commission (“FTC”) has promulgated numerous guides for
3 businesses which highlight the importance of implementing reasonable data security practices.
4 According to the FTC, the need for data security should be factored into all business decision-
5 making.
6

7 82. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide*
8 *for Business*, which established cyber-security guidelines for businesses. These guidelines note
9 that businesses should protect the personal consumer information that they keep; properly dispose
10 of personal information that is no longer needed; encrypt information stored on computer
11 networks; understand their network’s vulnerabilities; and implement policies to correct any
12 security problems.³⁰
13

14 83. The guidelines also recommend that businesses use an intrusion detection system
15 to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone
16 is attempting to hack the system; watch for large amounts of data being transmitted from the
17 system; and have a response plan ready in the event of a breach.³¹
18

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

25 _____
26 ³⁰ *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-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)
28 [personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)

³¹ *Id.*

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

8 86. These FTC enforcement actions include actions against financial services
9 companies, like Defendant.

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

16 88. Defendant failed to properly implement basic data security practices.

17 89. Defendant's failure to employ reasonable and appropriate measures to protect
18 against unauthorized access to the PII of its customers or to comply with applicable industry
19 standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. §
20 45.
21

22 90. Upon information and belief, Defendant was at all times fully aware of its
23 obligation to protect the PII of its customers, Defendant was also aware of the significant
24 repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was
25 particularly unreasonable given the nature and amount of PII it obtained and stored and the
26 foreseeable consequences of the immense damages that would result to Plaintiff and the Class.
27
28

1 ***Defendant Violated The Gramm-Leach-Bliley Act***

2 91. Defendant is a financial institution, as that term is defined by Section 509(3)(A) of
3 the Gramm-Leach-Bliley Act (“GLBA”), 15 U.S.C. § 6809(3)(A), and thus is subject to the
4 GLBA.

5 92. The GLBA defines a financial institution as “any institution the business of which
6 is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding
7 Company Act of 1956].” 15 U.S.C. § 6809(3)(A).

8 93. Defendant collects nonpublic personal information, as defined by 15 U.S.C. §
9 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant
10 time period Defendant were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et*
11 *seq.*, and is subject to numerous rules and regulations promulgated on the GLBA statutes.
12

13 94. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313.
14 Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for
15 implementing the Privacy Rule. In December 2011, the CFPB restated the implementing
16 regulations in an interim final rule that established the Privacy of Consumer Financial Information,
17 Regulation P, 12 C.F.R. § 1016 (“Regulation P”), with the final version becoming effective on
18 October 28, 2014.
19

20 95. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to
21 December 30, 2011 and by Regulation P after that date.
22

23 96. Both the Privacy Rule and Regulation P require financial institutions to provide
24 customers with an initial and annual privacy notice. These privacy notices must be “clear and
25 conspicuous.” 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. “Clear and
26 conspicuous means that a notice is reasonably understandable and designed to call attention to the
27
28

1 nature and significance of the information in the notice.” 16 C.F.R. § 313.3(b)(1); 12 C.F.R. §
2 1016.3(b)(1). These privacy notices must “accurately reflect[] [the financial institution’s] privacy
3 policies and practices.” 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must
4 include specified elements, including the categories of nonpublic personal information the
5 financial institution collects and discloses, the categories of third parties to whom the financial
6 institution discloses the information, and the financial institution’s security and confidentiality
7 policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6.
8 These privacy notices must be provided “so that each consumer can reasonably be expected to
9 receive actual notice.” 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant
10 violated the Privacy Rule and Regulation P.
11

12 97. Defendant failed to provide annual privacy notices to customers after the customer
13 relationship ended, despite retaining these customers’ PII and storing that PII on Defendant’s
14 network systems.
15

16 98. Defendant failed to adequately inform their customers that they were storing and/or
17 sharing, or would store and/or share, the customers’ PII on an insecure platform, accessible to
18 unauthorized parties from the internet, and would do so after the customer relationship ended.
19

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

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

7
8 100. As alleged herein, Defendant violated the Safeguard Rule.

9 101. Defendant failed to assess reasonably foreseeable risks to the security,
10 confidentiality, and integrity of customer information.

11 102. Defendant violated the GLBA and its own policies and procedures by sharing the
12 PII of Plaintiff and Class Members with a non-affiliated third party without providing Plaintiff and
13 Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

14
15 ***Defendant Fails To Comply With Industry Standards***

16 103. As noted above, experts studying cyber security routinely identify financial
17 services companies in possession of PII as being particularly vulnerable to cyberattacks because
18 of the value of the PII which they collect and maintain.

19 104. Several best practices have been identified that, at a minimum, should be
20 implemented by financial services companies in possession of PII, like Defendant, including but
21 not limited to: educating all employees; strong passwords; multi-layer security, including firewalls,
22 anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-
23 factor authentication; backup data and limiting which employees can access sensitive data.
24 Defendant failed to follow these industry best practices, including a failure to implement multi-
25 factor authentication.
26
27
28

1 105. Other best cybersecurity practices that are standard for financial services companies
2 include installing appropriate malware detection software; monitoring and limiting the network
3 ports; protecting web browsers and email management systems; setting up network systems such
4 as firewalls, switches and routers; monitoring and protection of physical security systems;
5 protection against any possible communication system; training staff regarding critical points.
6 Defendant failed to follow these cybersecurity best practices, including failure to train staff.
7

8 106. Defendant failed to meet the minimum standards of any of the following
9 frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation
10 PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR.DS-02,
11 PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06,
12 DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS
13 CSC), which are all established standards in reasonable cybersecurity readiness.
14

15 107. These foregoing frameworks are existing and applicable industry standards for
16 financial services companies, and upon information and belief, Defendant failed to comply with
17 at least one—or all—of these accepted standards, thereby opening the door to the threat actor and
18 causing the Data Breach.

19 ***Common Injuries & Damages***

20 108. As a result of Defendant's ineffective and inadequate data security practices, the
21 Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals,
22 the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and
23 Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion
24 of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity
25 costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss
26
27
28

1 of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the
2 actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and
3 certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized
4 third parties to access and abuse; and (b) remains backed up in Defendant's possession and is
5 subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and
6 adequate measures to protect the PII.
7

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

9 109. The unencrypted PII of Class Members will end up for sale on the dark web as that
10 is the *modus operandi* of hackers.
11

12 110. Unencrypted PII may also fall into the hands of companies that will use the detailed
13 PII for targeted marketing without the approval of Plaintiff and Class Members. Simply put,
14 unauthorized individuals can easily access the PII of Plaintiff and Class Members.
15

16 111. The link between a data breach and the risk of identity theft is simple and well
17 established. Criminals acquire and steal PII to monetize the information. Criminals monetize the
18 data by selling the stolen information on the black market to other criminals who then utilize the
19 information to commit a variety of identity theft related crimes discussed below.
20

21 112. Plaintiff's and Class Members' PII is of great value to hackers and cyber criminals,
22 and the data stolen in the Data Breach has been used and will continue to be used in a variety of
23 sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.
24

25 113. Due to the risk of one's Social Security number being exposed, state legislatures
26 have passed laws in recognition of the risk: "[t]he social security number can be used as a tool to
27 perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial
28 information, the release of which could cause great financial or personal harm to an individual.
29

1 While the social security number was intended to be used solely for the administration of the
2 federal Social Security System, over time this unique numeric identifier has been used extensively
3 for identity verification purposes[.]”³²

4 114. Moreover, “SSNs have been central to the American identity infrastructure for
5 years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into
6 their identification process for years. In fact, SSNs have been the gold standard for identifying and
7 verifying the credit history of prospective customers.”³³

8 115. “Despite the risk of fraud associated with the theft of Social Security numbers, just
9 five of the nation’s largest 25 banks have stopped using the numbers to verify a customer’s identity
10 after the initial account setup[.]”³⁴ Accordingly, since Social Security numbers are frequently used
11 to verify an individual’s identity after logging onto an account or attempting a transaction,
12 “[h]aving access to your Social Security number may be enough to help a thief steal money from
13 your bank account”³⁵

14 116. One such example of criminals piecing together bits and pieces of compromised
15 PII for profit is the development of “Fullz” packages.³⁶

16
17
18
19 ³² See N.C. Gen. Stat. § 132-1.10(1).

20 ³³ See <https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers>

21 ³⁴ See <https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/>

22 ³⁵ See <https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>

23
24 ³⁶ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not
25 limited to, the name, address, credit card information, social security number, date of birth, and
26 more. As a rule of thumb, the more information you have on a victim, the more money that can be
27 made off of those credentials. Fullz are usually pricier than standard credit card credentials,
28 commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning
credentials into money) in various ways, including performing bank transactions over the phone

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

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

11 119. The existence and prevalence of “Fullz” packages means that the PII stolen from
12 the data breach can easily be linked to the unregulated data (like contact information) of Plaintiff
13 and the other Class Members.

14 120. Thus, even if certain information (such as contact information) was not stolen in
15 the data breach, criminals can still easily create a comprehensive “Fullz” package.

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

18
19
20
21
22
23 with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials
24 associated with credit cards that are no longer valid, can still be used for numerous purposes,
25 including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule
26 account” (an account that will accept a fraudulent money transfer from a compromised account)
27 without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground*
28 *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/>)

Loss Of Time To Mitigate Risk Of Identity Theft & Fraud

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

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

124. Plaintiff’s mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”³⁷

125. Plaintiff’s mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.³⁸

³⁷ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

³⁸ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

1 126. And for those Class Members who experience actual identity theft and fraud, the
2 United States Government Accountability Office released a report in 2007 regarding data breaches
3 (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and
4 time to repair the damage to their good name and credit record.”⁴⁴

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

7 127. PII is a valuable property right.³⁹ Its value is axiomatic, considering the value of
8 Big Data in corporate America and the consequences of cyber thefts include heavy prison
9 sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has
10 considerable market value.

11 128. Sensitive PII can sell for as much as \$363 per record according to the Infosec
12 Institute.⁴⁰

13 129. An active and robust legitimate marketplace for PII also exists. In 2019, the data
14 brokering industry was worth roughly \$200 billion.⁴¹

15 130. In fact, the data marketplace is so sophisticated that consumers can actually sell
16 their non-public information directly to a data broker who in turn aggregates the information and
17 provides it to marketers or app developers.^{42,43}

18
19
20
21
22 ³⁹ 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 ⁴⁰ 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 ⁴¹ 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 ⁴² <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

28 ⁴³ <https://datacoup.com/>

1 131. Consumers who agree to provide their web browsing history to the Nielsen
2 Corporation can receive up to \$50.00 a year.⁴⁴

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

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

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

18 135. Plaintiff and Class Members now face years of constant surveillance of their
19 financial and personal records, monitoring, and loss of rights. The Class is incurring and will
20 continue to incur such damages in addition to any fraudulent use of their PII.
21

22 136. Defendant was, or should have been, fully aware of the unique type and the
23 significant volume of data on Defendant's network, amounting to, upon information and belief,
24 hundreds of thousands of individuals' detailed personal information and, thus, the significant
25 number of individuals who would be harmed by the exposure of the unencrypted data.
26

27 ⁴⁴ <https://digi.me/what-is-digime/>
28

1 137. The injuries to Plaintiff and Class Members were directly and proximately caused
2 by Defendant's failure to implement or maintain adequate data security measures for the PII of
3 Plaintiff and Class Members.

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

5 138. Given the type of targeted attack in this case, sophisticated criminal activity, and
6 the type of PII involved, there is a strong probability that entire batches of stolen information have
7 been placed, or will be placed, on the black market/dark web for sale and purchase by criminals
8 intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in the victims’
9 names to make purchases or to launder money; file false tax returns; take out loans or lines of
10 credit; or file false unemployment claims.
11

12 139. Such fraud may go undetected until debt collection calls commence months, or even
13 years, later. An individual may not know that his or her PII was used to file for unemployment
14 benefits until law enforcement notifies the individual’s employer of the suspected fraud.
15 Fraudulent tax returns are typically discovered only when an individual’s authentic tax return is
16 rejected.
17

18 140. Consequently, Plaintiff and Class Members are at an increased risk of fraud and
19 identity theft for many years into the future.
20

21 141. The retail cost of credit monitoring and identity theft monitoring can cost around
22 \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class
23 Members from the risk of identity theft that arose from Defendant's Data Breach.

24 ***Loss Of Benefit Of The Bargain***

25 142. Furthermore, Defendant’s poor data security practices deprived Plaintiff and Class
26 Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for
27
28

1 financial services, Plaintiff and other reasonable consumers understood and expected that they
2 were, in part, paying for the service and necessary data security to protect the PII, when in fact,
3 Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members
4 received services that were of a lesser value than what they reasonably expected to receive under
5 the bargains they struck with Defendant.
6

7 ***Plaintiff Tyrone Hammonds's Experience***

8 143. Plaintiff Tyrone Hammonds is a customer of Defendant's.

9 144. As a condition of obtaining financial services at Defendant, he was required to
10 provide his PII to Defendant.

11 145. Upon information and belief, at the time of the Data Breach, Defendant maintained
12 Plaintiff's PII in its system.

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

18 147. Upon information and belief, Plaintiff's PII was targeted, accessed, and acquired in
19 the Data Breach.
20

21 148. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the
22 impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach.
23 Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise
24 would have spent on other activities, including but not limited to work and/or recreation. This time
25 has been lost forever and cannot be recaptured.
26
27
28

1 149. Plaintiff suffered actual injury from having his PII compromised as a result of the
2 Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or
3 diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate
4 the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity
5 costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii)
6 nominal damages; and (viii) the continued and certainly increased risk to his PII, which: (a)
7 remains unencrypted and available for unauthorized third parties to access and abuse; and (b)
8 remains backed up in Defendant's possession and is subject to further unauthorized disclosures so
9 long as Defendant fails to undertake appropriate and adequate measures to protect the PII.
10

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

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

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

19 153. Plaintiff Tyrone Hammonds has a continuing interest in ensuring that his PII,
20 which, upon information and belief, remains backed up in Defendant's possession, is protected
21 and safeguarded from future breaches.
22

23 **CLASS ALLEGATIONS**

24 154. Plaintiff brings this nationwide class action on behalf of himself and on behalf of
25 all others similarly situated, pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4)
26 and/or 23(c)(5).
27
28

1 155. The Class that Plaintiff seeks to represent is defined as follows:

2 **Nationwide Class**

3 All individuals residing in the United States whose PII was accessed and/or
4 acquired by an unauthorized party as a result of the data breach that occurred at
5 Defendant in or about October 2024 (the “Class”).

6 156. Excluded from the Class are the following individuals and/or entities: Defendant
7 and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which
8 Defendant have a controlling interest; all individuals who make a timely election to be excluded
9 from this proceeding using the correct protocol for opting out; and all judges assigned to hear any
10 aspect of this litigation, as well as their immediate family members.

11 157. Plaintiff reserves the right to amend the definitions of the Class or add a Class or
12 Subclass if further information and discovery indicate that the definitions of the Class should be
13 narrowed, expanded, or otherwise modified.

14 158. Numerosity: The members of the Class are so numerous that joinder of all members
15 is impracticable, if not completely impossible. Although the precise number of individuals is
16 currently unknown to Plaintiff and exclusively in the possession of Defendant, upon information
17 and belief, thousands of individuals were impacted. The Class is apparently identifiable within
18 Defendant's records, and Defendant has already identified these individuals (as evidenced by
19 sending them breach notification letters).
20

21 159. Common questions of law and fact exist as to all members of the Class and
22 predominate over any questions affecting solely individual members of the Class. Among the
23 questions of law and fact common to the Class that predominate over questions which may affect
24 individual Class members, including the following:

- 25 a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and
26 Class Members;
27
28

- b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Plaintiff and Class Members are entitled to actual damages and/or nominal damages as a result of Defendant's wrongful conduct;
- k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

160. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

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

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

16 163. Superiority and Manageability: The class litigation is an appropriate method for fair
17 and efficient adjudication of the claims involved. Class action treatment is superior to all other
18 available methods for the fair and efficient adjudication of the controversy alleged herein; it will
19 permit a large number of Class Members to prosecute their common claims in a single forum
20 simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and
21 expense that hundreds of individual actions would require. Class action treatment will permit the
22 adjudication of relatively modest claims by certain Class Members, who could not individually
23 afford to litigate a complex claim against large corporations, like Defendant. Further, even for
24 those Class Members who could afford to litigate such a claim, it would still be economically
25 impractical and impose a burden on the courts.
26
27
28

1 164. The nature of this action and the nature of laws available to Plaintiff and Class
2 Members make the use of the class action device a particularly efficient and appropriate procedure
3 to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would
4 necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm
5 the limited resources of each individual Class Member with superior financial and legal resources;
6 the costs of individual suits could unreasonably consume the amounts that would be recovered;
7 proof of a common course of conduct to which Plaintiff was exposed is representative of that
8 experienced by the Class and will establish the right of each Class Member to recover on the cause
9 of action alleged; and individual actions would create a risk of inconsistent results and would be
10 unnecessary and duplicative of this litigation.
11

12 165. The litigation of the claims brought herein is manageable. Defendant's uniform
13 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class
14 Members demonstrates that there would be no significant manageability problems with
15 prosecuting this lawsuit as a class action.
16

17 166. Adequate notice can be given to Class Members directly using information
18 maintained in Defendant's records.
19

20 167. Unless a Class-wide injunction is issued, Defendant may continue in its failure to
21 properly secure the PII of Class Members, Defendant may continue to refuse to provide proper
22 notification to Class Members regarding the Data Breach, and Defendant may continue to act
23 unlawfully as set forth in this Complaint.

24 168. Further, Defendant has acted on grounds that apply generally to the Class as a
25 whole, so that class certification, injunctive relief, and corresponding declaratory relief are
26 appropriate on a class- wide basis.
27
28

1 169. Likewise, particular issues are appropriate for certification because such claims
2 present only particular, common issues, the resolution of which would advance the disposition of
3 this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- 4 a. Whether Defendant failed to timely notify the Plaintiff and the class of the Data
5 Breach;
6
7 b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care
8 in collecting, storing, and safeguarding their PII;
9
10 c. Whether Defendant's security measures to protect their data systems were
11 reasonable in light of best practices recommended by data security experts;
12
13 d. Whether Defendant's failure to institute adequate protective security measures
14 amounted to negligence;
15
16 e. Whether Defendant failed to take commercially reasonable steps to safeguard
17 consumer PII; and Whether adherence to FTC data security recommendations, and
18 measures recommended by data security experts would have reasonably prevented
19 the Data Breach.

20 **CAUSES OF ACTION**

21 **COUNT I**

22 **Negligence**

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

24 170. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if
25 fully set forth herein.

26 171. Defendant requires its customers, including Plaintiff and Class Members, to submit
27 non-public PII in the ordinary course of providing its financial services.
28

1 172. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its
2 business of soliciting its services to its customers, which solicitations and services affect
3 commerce.

4 173. Plaintiff and Class Members entrusted Defendant with their PII with the
5 understanding that Defendant would safeguard their information.
6

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

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

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

22 177. Defendant's duty to use reasonable security measures also arose under the GLBA,
23 under which they were required to protect the security, confidentiality, and integrity of customer
24 information by developing a comprehensive written information security program that contains
25 reasonable administrative, technical, and physical safeguards.
26
27
28

1 178. Defendant owed a duty of care to Plaintiff and Class Members to provide data
2 security consistent with industry standards and other requirements discussed herein, and to ensure
3 that its systems and networks adequately protected the PII.

4 179. Defendant's duty of care to use reasonable security measures arose as a result of the
5 special relationship that existed between Defendant and Plaintiff and Class Members. That special
6 relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII,
7 a necessary part of being customers at Defendant.
8

9 180. Defendant's duty to use reasonable care in protecting confidential data arose not
10 only as a result of the statutes and regulations described above, but also because Defendant is
11 bound by industry standards to protect confidential PII.
12

13 181. Defendant was subject to an "independent duty," untethered to any contract
14 between Defendant and Plaintiff or the Class.

15 182. Defendant also had a duty to exercise appropriate clearinghouse practices to remove
16 former customers' PII it was no longer required to retain pursuant to regulations.

17 183. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and
18 the Class of the Data Breach.

19 184. Defendant had and continues to have a duty to adequately disclose that the PII of
20 Plaintiff and the Class within Defendant's possession might have been compromised, how it was
21 compromised, and precisely the types of data that were compromised and when. Such notice was
22 necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity
23 theft and the fraudulent use of their PII by third parties.
24

25 185. Defendant breached its duties, pursuant to the FTC Act, GLBA, and other
26 applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class
27
28

1 Members' PII. The specific negligent acts and omissions committed by Defendant include, but are
2 not limited to, the following:

- 3 a. Failing to adopt, implement, and maintain adequate security measures to safeguard
4 Class Members' PII;
- 5 b. Failing to adequately monitor the security of their networks and systems;
- 6 c. Allowing unauthorized access to Class Members' PII;
- 7 d. Failing to detect in a timely manner that Class Members' PII had been
8 compromised;
- 9 e. Failing to remove former customers' PII it was no longer required to retain pursuant
10 to regulations, and
- 11 f. Failing to timely and adequately notify Class Members about the Data Breach's
12 occurrence and scope, so that they could take appropriate steps to mitigate the
13 potential for identity theft and other damages.

14
15
16 186. Defendant violated Section 5 of the FTC Act and GLBA by failing to use
17 reasonable measures to protect PII and not complying with applicable industry standards, as
18 described in detail herein. Defendant's conduct was particularly unreasonable given the nature and
19 amount of PII it obtained and stored and the foreseeable consequences of the immense damages
20 that would result to Plaintiff and the Class.

21
22 187. Plaintiff and Class Members were within the class of persons the Federal Trade
23 Commission Act and GLBA were intended to protect and the type of harm that resulted from the
24 Data Breach was the type of harm that the statutes were intended to guard against.

25 188. Defendant's violation of Section 5 of the FTC Act and GLBA constitutes
26 negligence.

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

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

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

11 192. Defendant has full knowledge of the sensitivity of the PII and the types of harm
12 that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

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

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

20 195. Plaintiff and the Class had no ability to protect their PII that was in, and possibly
21 remains in, Defendant's possession.

22 196. Defendant was in a position to protect against the harm suffered by Plaintiff and
23 the Class as a result of the Data Breach.

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

8 198. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost
9 and disclosed to unauthorized third persons as a result of the Data Breach.

10 199. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and
11 the Class, the PII of Plaintiff and the Class would not have been compromised.
12

13 200. There is a close causal connection between Defendant's failure to implement
14 security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent
15 harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed
16 as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII
17 by adopting, implementing, and maintaining appropriate security measures.

18 201. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class
19 have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft
20 of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated
21 with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the
22 bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences
23 of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to
24 their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and
25 abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized
26
27
28

1 disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect
2 the PII.

3 202. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff
4 and the Class have suffered and will suffer the continued risks of exposure of their PII, which
5 remain in Defendant's possession and is subject to further unauthorized disclosures so long as
6 Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued
7 possession.
8

9 203. Plaintiff and Class Members are entitled to compensatory and consequential
10 damages suffered as a result of the Data Breach.

11 204. Plaintiff and Class Members are also entitled to injunctive relief requiring
12 Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to
13 future annual audits of those systems and monitoring procedures; and (iii) continue to provide
14 adequate credit monitoring to all Class Members.
15

16 **COUNT II**
17 **Breach Of Implied Contract**
18 **(On Behalf of Plaintiff and the Class)**

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

21 206. Plaintiff and Class Members were required deliver their PII to Defendant as part of
22 the process of obtaining products or services provided by Defendant. Plaintiff and Class Members
23 paid money, or money was paid on their behalf, to Defendant in exchange for products or services
24 and would not have paid for Defendant's products or services, or would have paid less for them,
25 had they known that Defendant's data security practices were substandard.
26
27
28

1 207. Defendant solicited, offered, and invited Class Members to provide their PII as part
2 of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's
3 offers and provided their PII to Defendant.

4 208. Defendant accepted possession of Plaintiff's and Class Members' PII for the
5 purpose of providing services to Plaintiff and Class Members.
6

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

11 210. In entering into such implied contracts, Plaintiff and Class Members reasonably
12 believed and expected that Defendant's data security practices complied with relevant laws and
13 regulations (including FTC and GLBA guidelines on data security) and were consistent with
14 industry standards.
15

16 211. Implicit in the agreement between Plaintiff and Class Members and the Defendant
17 to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take
18 reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide
19 Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access
20 and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members
21 from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such
22 information secure and confidential.
23

24 212. The mutual understanding and intent of Plaintiff and Class Members on the one
25 hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.
26
27
28

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

5 214. On information and belief, Defendant further promised to comply with industry
6 standards and to make sure that Plaintiff's and Class Members' PII would remain protected.
7

8 215. Plaintiff and Class Members paid money to Defendant with the reasonable belief
9 and expectation that Defendant would use part of its earnings to obtain adequate data security.
10 Defendant failed to do so.

11 216. Plaintiff and Class Members would not have entrusted their PII to Defendant in the
12 absence of the implied contract between them and Defendant to keep their information reasonably
13 secure.
14

15 217. Plaintiff and Class Members would not have entrusted their PII to Defendant in the
16 absence of their implied promise to monitor their computer systems and networks to ensure that it
17 adopted reasonable data security measures.

18 218. Every contract in this State has an implied covenant of good faith and fair dealing,
19 which is an independent duty and may be breached even when there is no breach of a contract's
20 actual and/or express terms.
21

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

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

1 Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to
2 them that personal information was compromised as a result of the Data Breach.

3 221. Defendant breached the implied covenant of good faith and fair dealing by failing
4 to maintain adequate computer systems and data security practices to safeguard PII, failing to
5 timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued
6 acceptance of PII and storage of other personal information after Defendant knew, or should have
7 known, of the security vulnerabilities of the systems that were exploited in the Data Breach.
8

9 222. As a direct and proximate result of Defendant's breach of the implied contracts,
10 Plaintiff and Class Members sustained damages, including, but not limited to: (i) invasion of
11 privacy; (ii) theft of their 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 Breach; (v) loss
13 of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the
14 actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and
15 certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized
16 third parties to access and abuse; and (b) remains backed up in Defendant's possession and is
17 subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and
18 adequate measures to protect the PII.
19

20 223. Plaintiff and Class Members are entitled to compensatory, consequential, and
21 nominal damages suffered as a result of the Data Breach.
22

23 224. Plaintiff and Class Members are also entitled to injunctive relief requiring
24 Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit
25 to future annual audits of those systems and monitoring procedures; and (iii) immediately provide
26 adequate credit monitoring to all Class Members.
27
28

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

1
2
3 225. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if
4 fully set forth herein.

5 226. Plaintiff brings this Count in the alternative to the breach of implied contract count
6 above.

7
8 227. Plaintiff and Class Members conferred a monetary benefit on Defendant.
9 Specifically, they paid Defendant and/or its agents for financial services and in so doing also
10 provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received
11 from Defendant the services that were the subject of the transaction and should have had their PII
12 protected with adequate data security.

13 228. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and
14 has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant
15 profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII for business
16 purposes.

17
18 229. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did
19 not fully compensate Plaintiff or Class Members for the value that their PII provided.

20 230. Defendant acquired the PII through inequitable record retention as it failed to
21 investigate and/or disclose the inadequate data security practices previously alleged.

22
23 231. If Plaintiff and Class Members had known that Defendant would not use adequate
24 data security practices, procedures, and protocols to adequately monitor, supervise, and secure
25 their PII, they would have entrusted their PII at Defendant or obtained services at Defendant.

26 232. Plaintiff and Class Members have no adequate remedy at law.
27
28

1 233. Defendant enriched itself by saving the costs it reasonably should have expended
2 on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead
3 of providing a reasonable level of security that would have prevented the hacking incident,
4 Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class
5 Members by utilizing cheaper, ineffective security measures and diverting those funds to its own
6 profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of
7 Defendant's decision to prioritize its own profits over the requisite security and the safety of their
8 PII.
9

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

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

24 236. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages
25 from Defendant and/or an order proportionally disgorging all profits, benefits, and other
26 compensation obtained by Defendant from its wrongful conduct. This can be accomplished by
27
28

1 establishing a constructive trust from which the Plaintiff and Class Members may seek restitution
2 or compensation.

3 237. Plaintiff and Class Members may not have an adequate remedy at law against
4 Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the
5 alternative to, other claims pleaded herein.
6

7 **COUNT IV**
8 **Violation of California’s Unfair Competition Law (“UCL”)**
9 **Unlawful Business Practice**
10 **Cal Bus. & Prof. Code § 17200, *et seq.***
11 **(On Behalf of Plaintiff and the Class)**

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

14 239. Defendant is a “person” defined by Cal. Bus. & Prof. Code § 17201.

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

17 241. Defendant’s “unfair” acts and practices include:

- 18 a. by utilizing cheaper, ineffective security measures and diverting those funds
19 to its own profit, instead of providing a reasonable level of security that
20 would have prevented the hacking incident;
- 21 b. failing to follow industry standard and the applicable, required, and
22 appropriate protocols, policies, and procedures regarding the encryption of
23 data;
- 24 c. failing to timely and adequately notify Class Members about the Data
25 Breach’s occurrence and scope, so that they could take appropriate steps to
26 mitigate the potential for identity theft and other damages;
- 27
- 28

1 d. Omitting, suppressing, and concealing the material fact that it did not
2 reasonably or adequately secure Plaintiff's and Class Members' personal
3 information; and

4 e. Omitting, suppressing, and concealing the material fact that it did not
5 comply with common law and statutory duties pertaining to the security and
6 privacy of Plaintiff's and Class Members' personal information.
7

8 242. Defendant has engaged in "unlawful" business practices by violating multiple laws,
9 including the FTC Act, 15 U.S.C. § 45, GLBA, and California common law.

10 243. Defendant's unlawful, unfair, and deceptive acts and practices include:

11 a. Failing to implement and maintain reasonable security and privacy
12 measures to protect Plaintiff's and Class Members' personal information,
13 which was a direct and proximate cause of the Data Breach;

14 b. Failing to identify foreseeable security and privacy risks, remediate
15 identified security and privacy risks, which was a direct and proximate
16 cause of the Data Breach;

17 c. Failing to comply with common law and statutory duties pertaining to the
18 security and privacy of Plaintiff's and Class Members' personal
19 information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and
20 GLBA, which was a direct and proximate cause of the Data Breach;

21 d. Misrepresenting that it would protect the privacy and confidentiality of
22 Plaintiff's and Class Members' personal information, including by
23 implementing and maintaining reasonable security measures; and

24 e. Misrepresenting that it would comply with common law and statutory duties
25
26
27
28

1 pertaining to the security and privacy of Plaintiff’s and Class Members’
2 personal information, including duties imposed by the FTC Act, 15 U.S.C.
3 § 45 and GLBA.

4 244. Defendant’s representations and omissions were material because they were likely
5 to deceive reasonable consumers about the adequacy of Defendant’s data security and ability to
6 protect the confidentiality of consumers’ personal information.

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

12 246. Defendant’s violations were, and are, willful, deceptive, unfair, and
13 unconscionable.

14 247. Plaintiff and Class Members have lost money and property as a result of
15 Defendant’s conduct in violation of the UCL, as stated herein and above.

16 248. By deceptively storing, collecting, and disclosing their personal information,
17 Defendant has taken money or property from Plaintiff and Class Members.

18 249. Defendant acted intentionally, knowingly, and maliciously to violate California’s
19 Unfair Competition Law, and recklessly disregarded Plaintiff’s and Class Members’ rights.

20 250. Plaintiff and Class Members seek all monetary and nonmonetary relief allowed by
21 law, including restitution of all profits stemming from Defendant’s unfair, unlawful, and fraudulent
22 business practices or use of their personal information; declaratory relief; reasonable attorneys’
23 relief.

1 fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other
2 appropriate equitable relief, including public injunctive relief.

3
4 **COUNT V**
5 **Violation of the California Consumer Privacy Act of 2018 ("CCPA")**
6 **Cal. Civ. Code § 1798, *et seq.***
7 **(On Behalf of Plaintiff and the California Subclass)**

8 251. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if
9 fully set forth herein, and brings this claim on behalf of himself and the California Subclass (the
10 "Class" for the purposes of this count).

11 252. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a),
12 creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically
13 provides:

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

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

23 (B) Injunctive or declaratory relief.

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

25 253. Defendant is a "business" under § 1798.140(b) in that it is a corporation organized
26 for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of
27 \$25 million.

28 254. Plaintiff and Class Members are covered "consumers" under § 1798.140(g) in that
they are natural persons who are California residents.

1 255. The personal information of Plaintiff and the Class Members at issue in this lawsuit
2 constitutes “personal information” under § 1798.150(a) and 1798.81.5, in that the personal
3 information Defendant collects and which was impacted by the cybersecurity attack includes an
4 individual’s first name or first initial and the individual’s last name in combination with one or
5 more of the following data elements, with either the name or the data elements not encrypted or
6 redacted: (i) Social Security number; (ii) Driver’s license number, California identification card
7 number, tax identification number, passport number, military identification number, or other
8 unique identification number issued on a government document commonly used to verify the
9 identity of a specific individual; (iii) account number or credit or debit card number, in combination
10 with any required security code, access code, or password that would permit access to an
11 individual’s financial account; (iv) medical information; (v) health insurance information; (vi)
12 unique biometric data generated from measurements or technical analysis of human body
13 characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.
14

15 256. Defendant knew or should have known that its computer systems and data security
16 practices were inadequate to safeguard the Class Members’ personal information and that the risk
17 of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable
18 security procedures and practices appropriate to the nature of the information to protect the
19 personal information of Plaintiff and the Class Members. Specifically, Defendant subjected
20 Plaintiff’s and the Class Members’ nonencrypted and nonredacted personal information to an
21 unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant’s violation of
22 the duty to implement and maintain reasonable security procedures and practices appropriate to
23 the nature of the information, as described herein.
24
25
26
27
28

1 257. As a direct and proximate result of Defendant’s violation of its duty, the
2 unauthorized access and exfiltration, theft, or disclosure of Plaintiff’s and Class Members’
3 personal information included exfiltration, theft, or disclosure through Defendant’s servers,
4 systems, and website, and/or the dark web, where hackers further disclosed the personal
5 identifying information alleged herein.
6

7 258. As a direct and proximate result of Defendant’s acts, Plaintiff and the Class
8 Members were injured and lost money or property, including but not limited to the loss of
9 Plaintiff’s and Class Members’ legally protected interest in the confidentiality and privacy of their
10 personal information, stress, fear, and anxiety, nominal damages, and additional losses described
11 above.
12

13 259. Section 1798.150(b) specifically provides that “[n]o [prefiling] notice shall be
14 required prior to an individual consumer initiating an action solely for actual pecuniary damages.”
15

16 260. On November 22, 2024, Plaintiff’s counsel sent a CCPA notice letter to
17 Defendant’s registered service agents via certified mail. As of the date of this filing, Defendant
18 has not cured the effects of the Data Breach, which would require retrieving the PII and securing
19 the PII from continuing and future use, within 30 days of delivery of such CCPA notice letter.
20 Thus, Plaintiff seeks actual damages and statutory damages of no less than \$100 and up to \$750
21 per customer record subject to the Data Breach on behalf of the California Subclass as authorized
22 by the CCPA.

23 261. Accordingly, Plaintiff and the Class Members by way of this complaint seek actual
24 pecuniary damages suffered as a result of Defendant’s violations described herein.
25
26
27
28

PRAYER FOR RELIEF

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

- A. For an Order certifying the Class, and appointing Plaintiff and his Counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
 - iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or

1 unauthorized use of their PII for Plaintiff's and Class Members' respective
2 lifetimes;

3 v. requiring Defendant to implement and maintain a comprehensive Information
4 Security Program designed to protect the confidentiality and integrity of the
5 PII of Plaintiff and Class Members;

6 vi. prohibiting Defendant from maintaining the PII of Plaintiff and Class
7 Members on a cloud-based database;

8 vii. requiring Defendant to engage independent third-party security
9 auditors/penetration testers as well as internal security personnel to conduct
10 testing, including simulated attacks, penetration tests, and audits on
11 Defendant's systems on a periodic basis, and ordering Defendant to promptly
12 correct any problems or issues detected by such third-party security auditors;
13

14 viii. requiring Defendant to engage independent third-party security auditors and
15 internal personnel to run automated security monitoring;

16 ix. requiring Defendant to audit, test, and train its security personnel regarding
17 any new or modified procedures;

18 x. requiring Defendant to segment data by, among other things, creating
19 firewalls and controls so that if one area of Defendant's network is
20 compromised, hackers cannot gain access to portions of Defendant's systems;

21 xi. requiring Defendant to conduct regular database scanning and securing
22 checks;

23 xii. requiring Defendant to establish an information security training program that
24 includes at least annual information security training for all employees, with
25
26
27
28

1 additional training to be provided as appropriate based upon the employees'
2 respective responsibilities with handling personal identifying information, as
3 well as protecting the personal identifying information of Plaintiff and Class
4 Members;

5
6 xiii. requiring Defendant to routinely and continually conduct internal training and
7 education, and on an annual basis to inform internal security personnel how to
8 identify and contain a breach when it occurs and what to do in response to a
9 breach;

10
11 xiv. requiring Defendant to implement a system of tests to assess its respective
12 employees' knowledge of the education programs discussed in the preceding
13 subparagraphs, as well as randomly and periodically testing employees'
14 compliance with Defendant's policies, programs, and systems for protecting
15 personal identifying information;

16
17 xv. requiring Defendant to implement, maintain, regularly review, and revise as
18 necessary a threat management program designed to appropriately monitor
19 Defendant's information networks for threats, both internal and external, and
20 assess whether monitoring tools are appropriately configured, tested, and
21 updated;

22
23 xvi. requiring Defendant to meaningfully educate all Class Members about the
24 threats that they face as a result of the loss of their confidential personal
25 identifying information to third parties, as well as the steps affected
26 individuals must take to protect himself;
27
28

- 1 xvii. requiring Defendant to implement logging and monitoring programs sufficient
2 to track traffic to and from Defendant's servers; and
3
4 xviii. for a period of 10 years, appointing a qualified and independent third party
5 assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate
6 Defendant's compliance with the terms of the Court's final judgment, to
7 provide such report to the Court and to counsel for the class, and to report any
8 deficiencies with compliance of the Court's final judgment;
- 9 D. For an award of damages, including actual, nominal, consequential, and punitive
10 damages, as allowed by law in an amount to be determined;
- 11 E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- 12 F. For prejudgment interest on all amounts awarded; and
- 13 G. Such other and further relief as this Court may deem just and proper.

14
15 **JURY TRIAL DEMANDED**

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

17
18 Dated: November 22, 2024

Respectfully Submitted,

19
20 By: /s/ John J. Nelson
21 John J. Nelson (SBN 317598)
22 **MILBERG COLEMAN BRYSON**
23 **PHILLIPS GROSSMAN, PLLC**
24 402 Broadway, Suite 1760
25 San Diego, CA 92101
26 Telephone: (858) 209-6941
27 Email: jnelson@milberg.com
28

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

Jeff Ostrow*
KOPELOWITZ OSTROW P.A.
1 West Las Olas Blvd., Ste. 500
Fort Lauderdale, FL 33301
Tele: 954-332-4200
ostrow@kolawyers.com

*Attorneys for Plaintiff and
The Proposed Class*

**Pro Hac Vice application forthcoming*