UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF NEW YORK

SAMUEL TSOU, on behalf of himself and all others similarly situated,

Plaintiff,

vs.

BETTERMENT LLC, and BETTERMENT HOLDINGS, INC.

Defendants.

Case No.: _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Samuel Tsou ("Plaintiff") brings this Class Action Complaint against Betterment LLC, and Betterment Holdings, Inc. (collectively herein "Betterment" or "Defendants") individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsel's investigation, and upon information and belief as to all other matters, as follows:

I. NATURE OF THE ACTION

1. This class action arises out of the recent data breach ("Data Breach") involving Betterment, a New York based company that provides financial advisory services, including securities brokerage, cash management and retirement planning.[1]

2. Plaintiff brings this Complaint against Defendants for their failure to properly secure and safeguard the personally identifiable information that it collected and maintained as

[1] *See* "Fintech firm Betterment confirms data breach after hackers send fake crypto scam to notification to users", *Tech Crunch* - https://techcrunch.com/2026/01/12/fintech-firm-betterment-confirms-data-breach-after-hackers-send-fake-crypto-scam-notification-to-users/ (last visited January 15, 2026).

part of its regular business practices, including Plaintiff's and Class Members' full name, email addresses, physical addresses, phone numbers, and full date of birth information (collectively defined herein as "PII" or "Private Information").[2]

3. On or about January 12, 2026, Plaintiff received a notice ("Notice") from Betterment which indicated that on or around January 9, 2026, Betterment was subjected to a Data Breach in which Private Information of Plaintiff and Class Members was subject to unauthorized access.[3]

4. The Notice identifies that upon discovery of the Data Breach, Betterment launched an investigation and confirmed that unauthorized parties were able to gain access to certain company systems using access credentials obtained through social engineering mechanisms. The Notice also identifies that Betterment was able to verify that unauthorized parties did in fact access Personal Information.

5. Betterment has also reported that cybercriminals were able to use the unauthorized access to send fraudulent sales solicitation emails, via Betterment's approved customer marketing/communication channels.[4]

6. Betterment also reported on their Data Breach update webpage that their website and mobile application was subject to disruptions on January 13, 2026 to a disrupted denial-of-services (DDoS) attack.[5] Despite including information on the DDoS attack on the Data Breach update webpage, Betterment has not expressly indicated the DDoS attack was precipitated by the same parties responsible for the Data Breach.

---

[2] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.
[3] Betterment Notice Communication
[4] https://www.betterment.com/customer-update last visited (January 15, 2026).
[5] *Id*.

7. Upon information and belief, customers are required to entrust Defendants with sensitive, non-public Private Information as a condition of receiving services, without which Defendants could not perform their regular business activities. Defendants retains this information for many years and even after the customer relationship has ended.

8. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

9. Defendants failed to adequately protect Plaintiff's and Class Members' Private Information. This unencrypted, unredacted Private Information was compromised due to Defendants' negligent and/or careless acts and omissions and its utter failure to protect Plaintiff's and Class Members' Private Information. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk of identity theft and fraud to victims of the Data Breach will remain for their respective lifetimes.

10. In breaching its duties to properly safeguard Plaintiff's and Class Members' Private Information and give them timely, adequate notice of the Data Breach's occurrence, Defendants' conduct amounts to negligence and/or recklessness and violates federal and state statutes.

11. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendants' failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendants' inadequate information security practices; (iii) safeguard Defendants' own marketing and communication channels; (iv) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents; and (v) appropriately train its

employees, business partners, and vendors in information security practices, including the risk of social engineering. Defendants' conduct amounts at least to negligence and violates federal and state statutes.

12. Plaintiff and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Betterment's possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

13. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Betterment's inadequate data security practices.

II. PARTIES

14. Plaintiff Samuel Tsou is a resident and citizen of California.

15. On or about January 16, 2026, pursuant to § 1798.150(b) of the CCPA, Plaintiff Tsou separately provided written notice to Defendant identifying the specific provisions of this title he alleges it has violated. If within 30 days of Plaintiff's written notice to Defendant it fails to "actually cure" its violations of Cal. Civ. Code § 1798.150(a) and provide "an express written statement that the

violations have been cured and that no further violations shall occur," Plaintiff will amend this complaint to also seek the greater of statutory damages in an amount no less than one hundred dollars ($100) and up to seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater, on behalf of the Class. See Cal. Civ. Code § 1798.150(b).

16. Defendant Betterment LLC provides automated investing, retirement, and cash management solutions to retail investors, small businesses, and financial advisors. Betterment LLC's principal place of business is located at 450 West 33rd Street, FL 11, New York, NY 10001.

17. Defendant Betterment Holdings, Inc is the parent company of Betterment LLC and other related entities and subsidiaries which provide various services in support of Betterment's suite of product and service offerings. Betterment Holdings, Inc is headquartered in New York, NY. Betterment's principal place of business is located at 450 West 33rd Street, FL 11, New York, NY 10001.

III. JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants, namely Plaintiff, a citizen of California.

19. This Court has personal jurisdiction over Defendants because their principal places of business are in this District, they regularly conduct business in this District, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

20. Venue is proper under 28 U.S.C § 1391(b)(1) because Defendants' principal place of business are in this District.

IV. FACTUAL ALLEGATIONS

A. Betterment's Business

21. Betterment is a New York financial services company with more than one million customers, and over sixty five (65) billion dollars of assets under management.[6]

22. Plaintiff and Class Members are current and former customers of Defendants.

23. In order to obtain services from Defendants, Plaintiffs and Class Members were required to provide Defendants with their sensitive and confidential Private Information, including their names, and birthdates.

24. Upon information and belief, the information held by Defendants in their systems at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

25. Upon information and belief, Defendants made promises and representations to its current and former customers including Plaintiff and Class Members, that the Private Information collected from them as a condition of providing services would be kept safe, confidential, that the privacy of that information would be maintained.

26. Plaintiff and Class Members provided their Private Information to Defendants with reasonable expectation, and on mutual understanding, that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

27. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members relied on the sophistication of Defendants to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information.

[6] *See Betterment* "About Us" - https://www.betterment.com/about (last visited January 16, 2026)

Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

28. Defendants had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendants have a legal duty to keep their clients' Private Information safe and confidential.

29. In the course of collecting Private Information from consumers, including Plaintiffs and Class Members, Betterment promised to provide confidentiality and adequate security for Private Information through its applicable Privacy Policy and in compliance with statutory privacy requirements applicable to its industry. Betterment was in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach. Betterment is aware of and had obligations created by FTCA, contract, industry standards, and common law to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information.

30. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

B. The Data Breach

31. On or about January 9, 2026, Betterment became aware that an unauthorized individual gained access to certain Betterment systems through social engineering. After an unspecified amount

of time, between the date they became aware and sent the Notice, the investigation determined that an unauthorized actor accessed the Betterment network and exfiltrated the data.[7]

32. Omitted from the Notice Letter were the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

33. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harm resulting from the Data Breach is severely diminished.

34. Omitted from the Notice and the Data Breach update webpage are the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

35. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff and Class Members ability to mitigate the harms resulting from the Data Breach is severely diminished.

[7] *Supra* n.3

36. Despite Defendants' intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice, including: a) that this Data Breach was the work of cybercriminals; b) unauthorized party gained access to a database containing client data.

37. To be clear — there are numerous issues surrounding Betterment's Data Breach, but the deficiencies in the statement exacerbate the circumstances for victims of the Data Breach: (1) Betterment fails to state whether it was able to contain or end the cybersecurity threat, leaving victims to fear whether the Private Information that Defendants continue to maintain is secure; and (2) Beyond a general statement, Betterment fails to state how the breach itself occurred. All of this information is vital to victims of a data breach, let alone a data breach of this magnitude, which occurred to a financial services company who is a fiduciary to its customers and maintains custody of their financial assets.

38. Moreover, in the Notice, Betterment failed to specify whether it undertook any efforts to contact the Class Members whose data was accessed and acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their data, whether Class Members should report their misuse to Betterment, and whether Betterment set up any mechanism for Class Members to report any misuse of their data.

39. Betterment did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed..

C. Data Breaches Are Preventable.

40. Defendants could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

41. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[8]

42. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, customers and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- 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 not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

[8] https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited January 16. 2026)

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units. [9]

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

Secure internet-facing assets

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

Thoroughly investigate and remediate alerts

Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

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

Build credential hygiene

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

Apply principle of least-privilege

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

Harden infrastructure

Use Windows Defender Firewall
Enable tamper protection

Id. at 3-4

> Enable cloud-delivered protection
> Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[10]

44. Given that Defendants were storing the sensitive Private Information of Plaintiff and Class Members, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

45. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of, upon information and belief, potentially more than one million individuals, including that of Plaintiff and Class Members.

D. Defendant Acquires, Collects, and Stores Private Information

46. As a condition of receiving services, Plaintiff and Class Members were required to give their sensitive and confidential Private Information to Betterment.

47. Defendants retain and stores this information and derive a substantial economic benefit from the Private Information that they collect. But for the collection of Plaintiff's and Class Members' Private Information, Betterment would be unable to provide its services.

48. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

49. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and

[10] See https://www.microsoft.com/en-us/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited January 15, 2026)

maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

50. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class Members.

E. Defendant Knew or Should Have Known of the Risk Because Companies in Possession of Private Information are Particularly Susceptible to Cyber Attacks.

51. Data thieves regularly target companies like Betterment due to the highly sensitive information that they custody. Defendants knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

52. Betterment's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store Private Information and other sensitive information (like Defendants), preceding the date of the breach.

53. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims.[11] The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points. The 2023 compromises represent a 78 percentage point increase over the previous year and a 72 percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.

54. In light of recent high profile data breaches at other industry leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB

[11] See 2023 Data Breach Annual Report, https://www.idtheficenter.org/wp-content/uploads/2024/01/ITRC 2023 (last visited January 15, 2026)

Management Services, Inc. (1 million records, February 2023), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

55. Additionally, as companies became more dependent on computer systems to run their business[12], e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[13]

56. As a custodian of Private Information, Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiff and Class members, and of the foreseeable consequences if their data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

57. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

58. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

59. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' server(s) and system(s), amounting to several individuals'

[12] https://www.federalreserve.govieconres/notes/feds -notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited January 15, 2026).
[13] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last visited January 15, 2026).

detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

60. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

61. The ramifications of Defendants' failure to keep secure the Private Information of Plaintiff and Class Members are long-lasting and severe. Once Private Information is stolen—fraudulent use of that information and damage to victims may continue for years.

62. As a company in possession of Private Information, Betterment knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach.

F. Value of Personally Identifying Information.

63. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employee benefit management company or taxpayer identification number."[14]

[14] 17 C.F.R. § 248.201 (2013).

64. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[15] For example, Personal Information can be sold at a price ranging from $40 to $200.[16] Criminals can also purchase access to entire company data breaches from $900 to $4,500.

65. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

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

66. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

G. Defendant Fails to Comply with FTC Guidelines

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

---

[15] *Id*
[16] "Your personal data is for sale on the dark web. Here's how much it costs", *Digital Trends*, Oct. 16, 2019, available at: https ://www.digitaltrends com/computing/personal-data-s old-on-the -dark-web-how-much-it-costs/ (last visited January 16, 2026).
[17] Report to Congressional Requesters, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited January 16, 2026).

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

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

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

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

72. These FTC enforcement actions include actions against companies like Defendants.

73. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses,

such as Defendants, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

74. Defendants failed to properly implement basic data security practices.

75. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

76. Upon information and belief, Defendants' were at all times fully aware of their obligation to protect the Private Information of their clients' and customers, Defendants were also aware of the significant repercussions that would result from their failure to do so. Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

H. Betterment Fails to Comply with Industry Standards.

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

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

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

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

81. These foregoing frameworks are existing and applicable industry standards in the media industry safeguarding their employees and customers' data, and upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

I. Common Injuries and Damages.

82. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time associated with attempting to mitigate the actual consequences of the Data Breach; (v)

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

J. The Data Breach Increases Victims' Risk of Identity Theft

83. The unencrypted Private Information of Plaintiff and Class Members will end up for sale on the dark web as that is the modus operandi of hackers.

84. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

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

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

87. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[18]

88. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

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

90. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like contact information) of Plaintiff and the other Class Members.

[18] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, 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 with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. See, e.g., Brian Krebs, Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm, Krebs on Security (Sep. 18, 2014), https ://kreb sonsecuritv.eotn/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in- underground-stolen-from-texas-life-insurance-finn/ (last visited November 23, 2025).

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

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

K. Loss of Time to Mitigate the Risk of Identity Theft and Fraud.

93. 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 Private Information 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.

94. Thus, due to the actual and imminent risk of identity theft, Betterment, in its Notice, instructs Plaintiff and Class Members to remain vigilant and to be cautious of unexpected communication, while also failing to provide adequate details of the Data Breach.

95. Defendants' suggestion to remain vigilant and exercise caution, while failing to provide adequate details of the Data Breach, essentially forces Plaintiff and Class Members to expend a significant amount of time attempting to gather necessary information. Plaintiff's and Class Members' time is highly valuable and irreplaceable, and accordingly, Plaintiff and Class Members suffered actual injury and damages in the form of lost time that they spent on mitigation activities in response to the Data Breach and at the direction of Betterment's Notice Letter.

96. 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, freezing their payment cards, contacting credit bureaus to place freezes on their accounts, and

monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect. 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.

97. 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.[19]

98. 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.

99. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office 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."

L. Diminution of Value of Private Information.

100. Private Information is a valuable property right.[20] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy

[19] 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. (last visited January 16, 2026).
[20] See "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited January 16, 2026) ("GAO Report").

prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

101. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[21]

102. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[22]

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

104. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendants' data security system was breached,

[21] See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3 -4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted). (last visited January 16, 2026).

[22] https://digi.me/what-is-digime/ (last visited January 16, 2026).

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

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

106. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

107. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' networks, amounting to, upon information and belief, potentially over a million persons detailed Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

108. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

M. Future Costs of Credit and Identity Theft Monitoring is Reasonable and Necessary

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

110. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for

unemployment benefits until law enforcement notifies the individual's employee-benefit management company of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

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

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

N. Loss of Benefit of the Bargain.

113. Furthermore, Defendants' poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to obtain, goods and/or services from Defendants under certain terms, Plaintiff and other reasonable individuals understood and expected that Defendants would properly safeguard and protect their Private Information, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiff and Class Members received services of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

O. Plaintiff Samuel Tsou's Experience

114. Plaintiff Tsou is a current customer of Betterment and has been a customer of Betterment for approximately two years.

115. Plaintiff Tsou is a resident of California.

116. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's Private Information in their systems.

117. Plaintiff Tsou is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

118. Plaintiff Tsou provided his Private Information to Defendant and trusted they would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

119. Plaintiff Tsou reasonably understood that in exchange for providing Defendant with his Private Information, they would employ adequate cybersecurity measures and protect his Private Information.

120. As a result of the Data Breach, and at the direction of Betterment's communications, including the Notice, Plaintiff has spent significant time on activities in response to the Data Breach, valuable time that Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

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

122. Upon information and belief following the Data Breach, Plaintiff has received spam communications intended to fraudulently financial information and/or misappropriate Plaintiff's financial resources.

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

124. Plaintiff Tsou has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

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

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

V. CLASS ACTION ALLEGATIONS

127. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

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

Nationwide Class: All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach, including those who received notice of the Data Breach (the "Nationwide Class").

129. Plaintiff also brings this class action on behalf of himself and on behalf of the following California state subclass:

California Subclass: All individuals residing in the California whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach, including those who received notice of the Data Breach (the "California Subclass")

130. The Nationwide Class and California Subclass shall be collectively referred to herein after as the "Class" unless otherwise specified.

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

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

133. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

134. Numerosity. The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiff and exclusively in the possession of Betterment, upon information and belief, at least hundreds of thousands of individuals were likely impacted. The Class is apparently identifiable within Betterment's records, and Betterment has already identified these individuals (as evidenced by sending them breach notification letters).

135. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions

of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendants had respective duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants had respective duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. Whether Defendants 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 Defendants 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 Defendants' wrongful conduct; and,

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.

136. 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.

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

138. Adequacy. Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered is typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

139. Superiority and Manageability. The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of

individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large companies, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

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

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

142. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

143. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to

provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

144. Further, Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

145. Likewise, particular issues under Rule 23(c)(2) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the Plaintiff and the class of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendants' failed to take commercially reasonable steps to safeguard its clients' Private Information; and,

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

VI. CAUSES OF ACTION

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

146. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 145, as if fully set forth herein.

147. Defendants require current and former customers, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of providing its services.

148. Defendants gathered and stored the Private Information of Plaintiff and Class Members as part of its business of soliciting its clients, which solicitations and services affect commerce.

149. Plaintiff and Class Members entrusted Defendants with their Private Information with the understanding that Defendants would safeguard their information.

150. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

151. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

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

153. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

154. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendants with their confidential Private Information, a necessary part of receiving services.

155. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

156. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Class.

157. Defendants also had a duty to exercise appropriate clearinghouse practices to remove Private Information they were no longer required to retain pursuant to regulations.

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

159. Defendants have and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

160. Defendants breached their duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

e. Failing to remove former Private Information it was no longer required to retain pursuant to regulations, and;

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

161. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

162. Defendants' violation of Section 5 of the FTC Act constitutes negligence.

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

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

165. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

166. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches targeting companies in possession of Private Information.

167. Defendants have full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

168. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendants' systems.

169. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

170. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendants' possession.

171. Defendants were in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

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

173. Betterment has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

174. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

175. There is a close causal connection between Defendants' failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

176. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain;

(vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information.

177. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

178. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

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

180. Defendants' negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

181. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants' to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

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

182. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 145, as if fully set forth herein.

183. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendants of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendants' duty.

184. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Private Information and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendants' systems.

185. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

186. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

187. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

188. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered or will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time associated with

attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information.

189. Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

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

190. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 145, as if fully set forth herein.

191. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they provided Defendants with their Private Information and labor/time. In exchange, Plaintiff and Class Members should have had their Private Information protected with adequate data security.

192. Defendants knew that Plaintiff and Class Members conferred a benefit upon them and has accepted and retained that benefit by accepting and retaining the labor and the Private Information entrusted to it. Defendants profited from Plaintiff's labor and retained data and used Plaintiff's and Class Members' Private Information for business purposes.

193. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

194. Defendants acquired the Private Information through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

195. If Plaintiff and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would not have entrusted their Private Information to Defendants.

196. Plaintiff and Class Members have no adequate remedy at law.

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

198. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

199. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) nominal damages; and (ix) the continued and certainly increased risk to their

Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

200. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

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

COUNT IV
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

202. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 145, as if fully set forth herein.

203. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

204. Defendants owed a duty to its current and former customers, including Plaintiff and the Class, to keep this information confidential.

205. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class members' Private Information is highly offensive to a reasonable person.

206. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendants, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

207. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

208. Defendants acted with a knowing state of mind when they permitted the Data Breach because they knew its information security practices were inadequate.

209. Defendants acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

210. Acting with knowledge, Defendants had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

211. As a proximate result of Defendants' acts and omissions, the private and sensitive Private Information of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed supra).

212. And, on information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

213. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information is still maintained by Defendants with their inadequate cybersecurity system and policies.

214. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendants' inability to safeguard Private Information of Plaintiff and the Class.

215. In addition to injunctive relief, Plaintiff, on behalf of himself and the other Class members, also seek compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

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

216. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 145, as if fully set forth herein.

217. Given the relationship between Defendants and Plaintiff and Class members, where Defendants became guardians of Plaintiff's and Class members' Private Information, Defendants became a fiduciary by their undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' Private Information; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants did and do store.

218. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendants' relationship with them—especially to secure their Private Information.

219. Because of the highly sensitive nature of the Private Information, Plaintiff and Class members (or their third-party agents) would not have entrusted Defendants, or anyone in Defendants' position, to retain their Private Information had they known the reality of Defendants' inadequate data security practices.

220. Defendants breached their fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' Private Information.

221. Defendants have also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

222. As a direct and proximate result of Defendants' breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed supra).

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

223. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 145, as if fully set forth herein.

224. Plaintiff and the Class entrusted their PII to Defendant as a condition of receiving services from Defendants. In so doing, Plaintiff and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

225. At the time Defendants acquired the PII of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendants would safeguard the PII and not take unjustified risks when storing the PII.

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

227. Plaintiff and the Class would not have entrusted their PII to Defendants had they known that Defendants would make the PII internet-accessible, not encrypt sensitive data elements, and not delete the PII that Defendants no longer had a reasonable need to maintain it.

228. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendants.

229. Defendants breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

230. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent

initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

231. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages to be determined at trial.

COUNT VII
VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200, et seq.
(On Behalf of Plaintiff and the Class)

232. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 145, as if fully set forth herein.

233. Defendants' acts and omissions as alleged herein emanated and directed from California.

234. By reason of the conduct alleged herein, Defendants engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq.*

235. Defendants stored the PII of Plaintiff and Class Members in its computer systems.

236. Defendants knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiff's and Class Members' PII secure and prevented the loss or misuse of that PII.

237. Defendants did not disclose at any time that Plaintiff's and Class Members' PII was vulnerable to hackers because Defendants' data security measures were inadequate and outdated, and Defendants were the only ones in possession of that material information, which Defendants had a duty to disclose.

A. **Unlawful Business Practices**

238. As noted above, Defendants violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, by omission, the safety of its computer systems, specifically the security thereof, and its ability to safely store Plaintiff's and Class Members' PII.

239. Defendants also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security.

240. If Defendants had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach, and consequently from Defendants' failure to timely notify Plaintiff and Class Members of the Data Breach.

241. Defendants' acts and omissions as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the FTC Act.

242. Plaintiff and Class Members suffered injury in fact and lost money or property as the result of Defendants' unlawful business practices. In addition, Plaintiff's and Class Members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

B. **Unfair Business Practices**

243. Defendants engaged in unfair business practices under the "balancing test." The harm caused by Defendants' actions and omissions, as described in detail above, greatly outweighs any perceived utility. Indeed, Defendants' failure to follow basic data security protocols and failure to disclose inadequacies of Defendants' data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiff and Class Members, directly causing the harms alleged below.

244. Defendants engaged in unfair business practices under the "tethering test." Defendants' actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them .... The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

245. Defendants engaged in unfair business practices under the "FTC test." The harm caused by Defendants' actions and omissions, as described in detail above, is substantial in that it affects thousands of Class Members and has caused those persons to suffer actual harm. Such harms include a substantial risk of identity theft, disclosure of Plaintiff's and Class Members' PII to third parties without their consent, diminution in value of their PII, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiff's and Class Members' PII remains in Defendants' possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendants' actions and omissions violated Section 5(a) of the Federal Trade Commission Act. See 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); *see also, e.g., In re*

LabMD, Inc., FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated §5(a) of FTC Act).

246. Plaintiff and Class Members suffered injury in fact and lost money or property as the result of Defendants' unfair business practices. Plaintiff's and Class Members' PII was taken and in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and Class Members have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

247. As a result of Defendants' unlawful and unfair business practices in violation of the UCL, Plaintiff and Class Members are entitled to damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT VIII
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. §§ 1798.100, *et. seq*. ("CCPA")
(On Behalf of Plaintiff and the California Subclass)

248. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 145, as if fully set forth herein.

249. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access and disclosure. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to

destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."

250. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendants failed to implement such procedures which resulted in the Data Breach.

251. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

252. Section 1798.150(a)(1) of the CCPA provides:

> "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper."

253. Plaintiff and California Subclass Members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

254. Defendants are a "business" as defined by Civ. Code § 1798.140(c) because Defendants:

a. are a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. Does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

255. The PII taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and California Subclass Members' includes, at least, certain names, email addresses, financial account information, physical addresses, phone numbers, and birthdates among other information.

256. Plaintiff and California Subclass Members' PII was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including name and contact information was wrongfully taken, accessed, and viewed by an unauthorized third party.

257. The Data Breach occurred as a result of Defendants' failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and California Subclass Members' PII. Defendants failed to implement reasonable security procedures to prevent an attack on their server or network, including its email system, by hackers and

to prevent unauthorized access of Plaintiff's and California Subclass Members' PII as a result of this attack.

258. On or about January 16, 2026, Plaintiff provided Defendants with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). If Defendants fails to respond, or have not cured, or are unable to cure the violation within 30 days thereof, Plaintiff will amend this Complaint to seek all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

259. As a result of Defendants' failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT IX
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

260. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 145, as if fully set forth herein.

261. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

262. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendants' common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiff alleges Defendants' actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class

continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

263. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants continue to owe a legal duty to employ reasonable data security to secure the Private Information it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendants continues to breach its duty by failing to employ reasonable measures to secure personal and financial information; and

c. Defendants' breach of its legal duty continues to cause harm to Plaintiff and the Class.

264. The Court should also issue corresponding injunctive relief requiring Defendants to employ adequate security protocols consistent with industry standards to protect Plaintiff's and the Class's data.

265. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendants' data systems. If another breach of Defendants' data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

266. The hardship to Plaintiff and the Class if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued.

267. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, request judgment against Defendants and that the Court grants the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to 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 Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants 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 Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants 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 Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendants from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be

provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendants to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess its clients' employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a S0C 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

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

E. For an award of attorneys' fees and costs as allowed by law;

F. For prejudgment interest on all amounts awarded; and

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

VIII. JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury on all claims so triable.

Dated: January 16, 2026

By: */s/ Alyssa Tolentino*

Alyssa Tolentino (Bar No. 6195481)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
atolentino@sirillp.com

Gregory Haroutunian (No. 5187430)
M. Anderson Berry*
Brook E. Garberding*
EMERY | REDDY, PC
600 Stewart Street, Suite 1100
Seattle, WA 98101
916.823.6955 (Tel)
206.441.9711 (Fax)
gregory@emeryreddy.com
anderson@emeryreddy.com
brook@emeryreddy.com

*Pro Hac Vice Forthcoming

Attorneys for Plaintiff