IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF CONNECTICUT

Mathis v. Planet Home Lending, LLC, (In re: Planet Home Lending, LLC Data Breach)	**Case No. 3:24-cv-00127-KAD** **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Brandon Mathis, Nashira Williams, Jaime Lee Mazzo, Jeffrey Benson, Frank Canepa, William Ekola, Joe Ward, Antonio Cole, and Ramsey Coulter ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this Consolidated Class Action Complaint against Defendant Planet Home Lending, LLC ("Defendant" or "Planet") and allege on information and belief, except as to their own actions, which are made on personal knowledge, the investigation of counsel, and the facts that are a matter of public record, as follows:

INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard Plaintiffs' and other similarly situated customers' sensitive information, including full names, addresses, Social Security numbers, loan numbers, and financial account numbers ("personally identifiable information" or "PII").

2. Defendant Planet is a financial services company based in Meriden, Connecticut. Planet specializes in residential home mortgages and refinances, offering homebuyers and existing homeowners various lending options. Planet employs more than 1,200 people and generates approximately $618 million in annual revenue.

3. According to reports, former and current customers at Planet are required to entrust

Defendant with sensitive, non-public PII, without which Defendant could not perform its regular business activities, in order to obtain products or services at Defendant. Defendant retains this information for at least many years and even after the customer relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On November 15, 2023, a Data Breach occurred as the result of "a vulnerability. . . existing in a software program that Planet purchased[.]"[1] Subsequently, Planet immediately initiated an investigation of the matter and engaged an outside forensic firm to assist with the process.[2] The investigation revealed that "the threat actor accessed a read-only data folder in which copies of loan files containing personally identifiable information of some of [Planet's] customers were stored."[3] On November 28, 2023, Defendant determined that certain personal data stored in the network environment, including the personally identifiable information of approximately 200,000 individuals, was accessible to the unauthorized actor.[4] Planet then took steps to provide notice to those individuals whose information was involved.[5]

6. According to Defendant's letter sent to Plaintiffs and other victims of the Notice of Data Breach (the "Notice Letter"), the compromised PII included individuals' full names, addresses, Social Security numbers, loan numbers, and financial account numbers.[6]

---

[1] The "Notice Letter." A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/5f9aa393-9c7a-49e0-855f-5e36adfb9e6c.shtml (last accessed Feb. 2, 2024).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*

7. Defendant failed to adequately protect Plaintiffs' and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and their utter failure to protect employee and customers' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

8. Plaintiffs brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

9. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

10. Plaintiffs and Class Members have suffered injury as a result of Defendant's

conduct. These injuries include: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs 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; and (vii) the continued and certainly increased risk to their PII, 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 PII.

11. Plaintiffs and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves 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 Defendant's inadequate data security practices.

PARTIES

12. Plaintiff Brandon Mathis is a resident of Florida.

13. Plaintiff Nashira Williams is a resident of Pennsylvania.

14. Plaintiff Jaime Lee Mazzo is a resident of Florida.

15. Plaintiff Jeffrey Benson is a resident of North Carolina.

16. Plaintiff Frank Canepa is a resident of New Jersey.

17. Plaintiff William Ekola is a resident of Arizona.

18. Plaintiff Joe Ward is a resident of Texas.

19. Plaintiff Antonio Cole is a resident of Alabama.

20. Plaintiff Ramsey Coulter is a resident of Florida.

21. Defendant Planet Home Lending, LLC is a Connecticut for-profit corporation that maintains its principal place of business at 321 Research Parkway, Suite 303, Meriden, Connecticut 06450.

JURISDICTION AND VENUE

22. The Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members significantly exceeds 1,000, many of whom have different citizenship from Defendant, including Plaintiffs. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

23. This Court has personal jurisdiction over Defendant because its principal place of business is in this District.

24. Venue is proper in this District because Defendant principal place of business is in this District and a significant amount of the events leading to Plaintiffs' causes of action occurred in this District.

FACTUAL ALLEGATIONS

Defendant's Business

25. Defendant is a financial services company based in Meriden, Connecticut. Planet specializes in residential home mortgages and refinances, offering homebuyers and existing homeowners lending options. Planet Home Lending employs more than 1,200 people and generates approximately $618 million in annual revenue.

26. Plaintiffs and Class Members are current and former customers of Defendant.

27. As a condition of receiving products and/or services from Defendant, Defendant requires that its customers, including Plaintiffs and Class Members, entrust it with highly sensitive personal information.

28. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted PII of Plaintiffs and Class Members.

29. Defendant made promises and representations to its customers, including Plaintiffs and Class Members, that the PII collected from them as a condition of obtaining products and/or services at Defendant would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it. Indeed, Defendant provides on its website, in part that:

> At Planet Home Lending, LLC, ("Planet"), we recognize your right to confidentiality and value your trust very seriously. We strive to protect the privacy of our clients' personal information and their customers' data. By publishing this Privacy Statement ("Statement"), we want you to know that we apply our long-standing commitment to safeguarding privacy to all of our online services and activities. This Statement discloses the privacy practices for www.planethomelending.com ("Website"). The use of this Website or the Services (as defined below), including the submission of data, constitutes your acknowledgement that you have read and understood this Statement and agreed with its terms. We reserve the right to change this Statement upon notification to you. Use of this site following provision of such notice shall constitute your acceptance of the revised terms.
>
> **Information Collection and User Registration**
>
> Any person accessing, browsing or otherwise using the Website, whether manually or through an automated mechanism is considered a "User". Planet collects information from two types of Users: casual Users, who may access the main site and non-restricted pages of the Website, and registered Users, or "Clients", who register with Planet and are thereby permitted to access the restricted pages of the Website.
>
> . . .
>
> **Use of Collected Information**
>
> Except as may otherwise be agreed in writing by Planet and any Client, whether in a contract for the provisions of Services (a "Services Agreement") or otherwise, which agreement will govern only data submitted to or gathered by Planet with respect to such Client, Planet is the sole owner of the information collected on the Website. We will not sell, share, or rent this information to others in ways different from what is disclosed in this Privacy Statement.

> Planet uses the information we collect to set up the Services for individuals. We may also use the information to contact clients and prospects to discuss further their interest in our Services and to provide information (such as announcements of promotions and events) about Planet or its partners.
>
> . . .
>
> **Security**
>
> Planet uses Secure Sockets Layer (SSL) encryption technology to keep your personal information as secure as possible. While we strive to protect your personal information, Planet cannot warrant or guarantee the security of any information you transmit.[7]

30. Plaintiffs and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

31. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

32. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's PII safe and confidential.

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

[7] "Consumer Privacy Notice", available at https://planethomelending.com/privacy-policy/ (last visited Feb. 2, 2024).

34. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

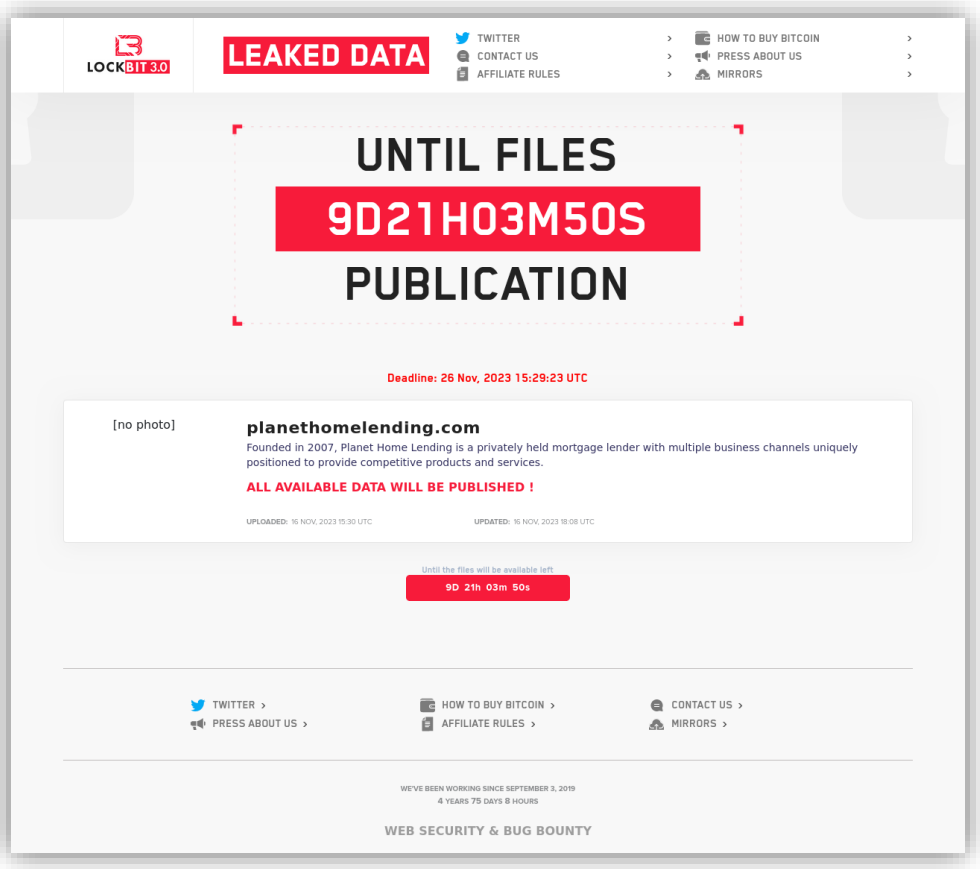
35. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

The Data Breach

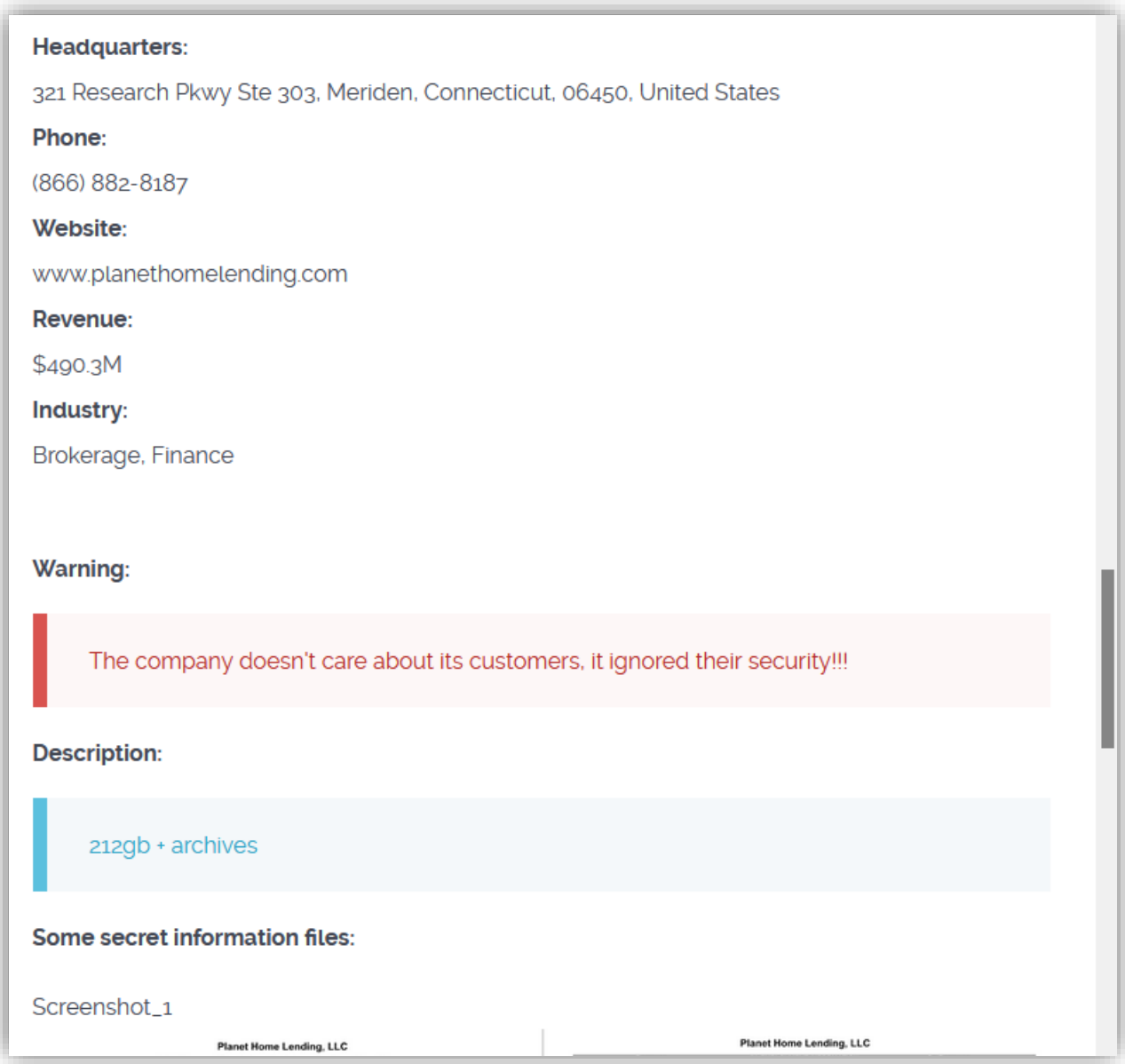
36. On or about January 24, 2023, Defendant began sending Plaintiffs and other victims of the Data Breach (the "Notice Letter"), informing them that:

> Planet Home Lending, LLC ("Planet") is writing to notify you of a recent incident that may affect the privacy of some of your personal information. Planet takes the protection of your information very seriously. Although we have no specific evidence of identity theft or fraud related to your information as a result of this incident, this letter provides information about the incident, our response, and steps you may wish to take to protect against misuse of your information.
>
> . . .
>
> The attack occurred on November 15, 2023, and Planet became aware of it that same day. Upon discovery, we took immediate action to contain the compromise and eradicate the threat. We also retained an experienced outside forensics firm to conduct a thorough investigation into the cause and impact of the breach, to confirm the attack had been contained and no additional unauthorized access had occurred, and to determine whether and to what extent any customer data may have been affected. On November 28, 2023, Planet was able to determine with reasonable certainty that the threat actor accessed a read-only data folder in which copies of loan files containing personally identifiable information of some of its customers were stored. Once we were able to make the determination that the data folder had been compromised, we worked diligently to thoroughly analyze the large volume of impacted data in order to determine the specific data elements and parties impacted. This notice has not been delayed as a result of a law enforcement investigation.
>
> **What Information Was Involved?** The investigation determined that certain of your personal information was present in the loan files that were compromised by the threat actor, including the following data elements: name, address, Social Security number, loan number, and financial account number.

37. Defendant does admit in the Notice Letter that the notorious LockBit ransomware gang claimed responsibility for the cyberattack. LockBit is one of the most active ransomware actors, having breached over 1,000 companies worldwide[8] on a "global ransomware campaign." Planet Home knew or should have known of the tactics that groups like LockBit employ.



[8] LockBit Hackers, BloomBerg, https://www.bloomberg.com/news/articles/2023-02-02/lockbit-hackers-behind-ion-breach-also-hit-royal-mail-hospital (last visited June 13, 2023).



Headquarters:

321 Research Pkwy Ste 303, Meriden, Connecticut, 06450, United States

Phone:

(866) 882-8187

Website:

www.planethomelending.com

Revenue:

$490.3M

Industry:

Brokerage, Finance

Warning:

The company doesn't care about its customers, it ignored their security!!!

Description:

212gb + archives

Some secret information files:

Screenshot_1

Planet Home Lending, LLC

Planet Home Lending, LLC

38. With the PII secured and stolen by Lockbit, the hackers then purportedly issued a ransom demand to Defendant. However, Defendant provided no public information on the ransom demand but admits in the Notice Letter that it has "not paid and do[es] not anticipate paying, any ransom amount to the threat actor."

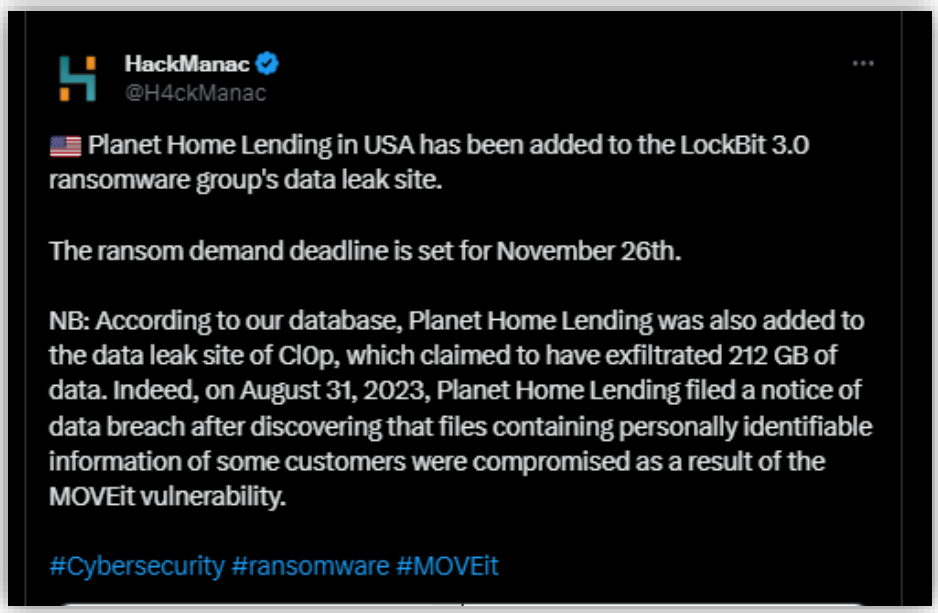
39. On information or belief, Lockbit is anticipated to release all stolen information onto the dark web for access, sale, and download following the deadline of the ransom demand to

Defendant.

40. Indeed, Lockbit has not only stated that it is going to release all stolen information onto the dark web for sale, but that Defendant's cybersecurity system was particularly abysmal, commenting "the company doesn't care about its customers. It ignored their security!"

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

42. Shockingly, Planet Home's cybersecurity systems and its supervision of its cybersecurity employees and agents are so abysmal that shortly before this Data Breach August 31, 2023, a *different* cybercriminal actor, Cl0p ransomware, stole 212 GB of data through a *different* cybersecurity vulnerability:



43. This tactic of exfiltrating the PII for a ransom demand before placing PII onto a

data leak page if the ransom demand is not met is something Lockbit and Cl0p, two of the most successful and lucrative ransomware gangs in the world, is well known for.[9] Defendants knew or should have known of the tactics that groups like Lockbit and Cl0p employ.

44. Despite having knowledge that at least one ransomware gang had accessed and stolen its clients' most sensitive and valuable information, Defendant did not begin notifying Class Members about the Data Breach until January 24, 2024–over two months after the Data Breach first occurred.

45. Despite its duties to safeguard PII, Defendant, a self-proclaimed leader in its industry, did not in fact follow industry standard practices in securing clients' PII, as evidenced by the Data Breach.

46. Despite the promises it makes to clients through its privacy policy, its cybersecurity practices were so insufficient that cybercriminals were able to bypass these protections.

47. Defendant further contends in its Notice Letter that it is or will "implement[] additional technical safeguards." Although Defendant fails to expand on what these "additional technical safeguards" are, such actions should have been in place before the Data Breach.

48. Through its Notice Letter, Defendant recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to be "vigilant against incidents of identity theft and fraud by reviewing your account statements, monitoring free credit reports you are entitled to receive, and immediately reporting any suspicious activity or incidents of suspected identity theft or fraud[.]"

49. Defendant further recognized its duty to implement reasonable cybersecurity

[9] Ransomware spotlight: Clop, Trendmicro, https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop (last visited October 17, 2023).

safeguards or policies to protect clients' PII, promising in its Notice Letter that, despite the Data Breach demonstrating otherwise, Defendant "take[s] the security of information in our care seriously."

50. On information and belief, Planet Home has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

51. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

52. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs' and the Class's financial accounts.

53. On information and belief, Planet Home failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its clients' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

Defendant Acquires, Collects, and Stores Its Customers' PII

54. As a condition to obtain products and/or services from Defendant, Plaintiffs and Class Members were required to give their sensitive and confidential PII to Defendant.

55. Defendant retains and stores this information and derives a substantial economic benefit from the PII that they collect. But for the collection of Plaintiffs' and Class Members' PII, Defendant would be unable to perform its services.

56. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

57. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

58. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and Class Members.

59. Defendant made promises to Plaintiffs and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

60. Indeed, Defendant provides on its website that:

> "All of our Users' information, not just the sensitive information mentioned above, is restricted in our offices. Only employees who need the information to perform a specific job are granted access to the information. Furthermore, all employees are kept up-to-date on our security and privacy practices. Any time new policies are added, our employees are notified and/or reminded about the importance we place on privacy, and what they can do to ensure that our Clients' and their customers' information is protected. Finally, the servers on which we store our Clients' data are kept in a secure environment, with around the clock security."[10]

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

[10] "Consumer Privacy Notice", available at https://planethomelending.com/privacy-policy/ (last visited Feb. 2, 2024).

Defendant Knew, Or Should Have Known, of the Risk Because Lending Companies in Possession of PII Are Particularly Susceptible to Cyber Attacks.

62. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they hold in their custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

63. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting lending companies that collect and store PII, like Defendant, preceding the date of the breach. According to the *2023 Annual Data Breach Report*, the number of data compromises in 2023 (3,205) increased by 78 percentage points compared to 2022 (1,801).[11] The ITRC set a new record for the number of data compromises tracked in a year, up 72 percentage points from the previous all-time high in 2021 (1,860).[12]

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

65. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report

[11] https://www.idtheftcenter.org/publication/2023-data-breach-report/
[12] *Id.*

explained, entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[13]

66. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

67. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

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

69. Additionally, as companies became more dependent on computer systems to run their business,[14] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of

[13] *FBI, Secret Service Warn Of Targeted Ransomware*, available at https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Feb. 2, 2024).

[14] *Implications of Cyber Risk for Financial Stability*, available at https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last accessed Feb. 2, 2024).

Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[15]

70. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousand individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

71. In the Notice Letter, Defendant offers to cover 24 months of identity monitoring for Plaintiffs and Class Members. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs and Class Members' PII. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

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

73. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

[15] *Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022*, available at https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last accessed Feb. 2, 2024).

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

75. As an institution in possession of its current and former customers' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems, or those on which it transferred PII, were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of PII

76. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[16] 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, employer or taxpayer identification number."[17]

77. The PII 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.[18]

[16] 17 C.F.R. § 248.201 (2013).
[17] *Id.*
[18] *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-sold-on-the-dark-web-how-much-it-costs/ (last visited Feb. 2, 2024).

78. For example, Personal Information can be sold at a price ranging from $40 to $200.[19] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[20]

79. For example, Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

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

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

81. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link

---

[19] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Feb. 2, 2024).

[20] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Feb. 2, 2024).

[21] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Feb. 2, 2024).

the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[22]

82. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number and name.

83. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[23]

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

85. 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 PII 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

[22] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Feb. 2, 2024).

[23] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Feb. 2, 2024).

> continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[24]

86. Plaintiffs 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 PII.

Defendant Fails to Comply with FTC Guidelines

87. 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.

88. 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 customer 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.[25]

89. 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.[26]

---

[24] *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited Jan. 17, 2024).
[25] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Feb. 2, 2024).
[26] *Id.*

90. The FTC further recommends that companies not maintain PII 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.

91. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer 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.

92. These FTC enforcement actions include actions against institutions like Defendant.

93. 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 Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

94. Defendant failed to properly implement basic data security practices.

95. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII 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.

96. Defendant was at all times fully aware of its obligation to protect the PII of its customers. Defendant was also aware of the significant repercussions that would result from its

failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendant Fails to Comply with Industry Standards

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

98. Several best practices have been identified that, at a minimum, should be implemented by lending companies in possession of PII, like Defendant, 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. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

99. Other best cybersecurity practices that are standard in the lending 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. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

100. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

101. These foregoing frameworks are existing and applicable industry standards in the lending industry and Defendant 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.

Common Injuries and Damages

102. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; (e) invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

The Data Breach Increases Victims' Risk of Identity Theft

103. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

104. The unencrypted PII of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs

and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

105. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII 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.

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

107. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or Phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

108. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[27]

[27] "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

109. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII 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.

110. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' 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 PII 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.

111. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiffs and the other Class Members

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

113. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to

---

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://krebsonsecuritv.eom/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 on Feb. 2, 2024).

crooked operators and other criminals (like illegal and scam telemarketers).

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

Loss Of Time to Mitigate Risk of Identity Theft and Fraud

115. Plaintiffs 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 upon receiving the Notice Letter.

116. Plaintiffs' 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."[28]

117. Plaintiffs' 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),

[28] *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 accessed Feb. 2, 2024).

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.[29]

118. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, 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 PII 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.

119. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

120. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[30] The information

[29] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed Feb. 2, 2024).

[30] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed Feb. 2, 2024).

disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

121. Consequently, Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

122. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Loss Of the Benefit of The Bargain

123. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant for products and/or services, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the service that provided the necessary data security to protect their PII, when in fact, Plaintiffs did not provide the expected data security. Accordingly, Plaintiffs and Class Members received products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff Brandon Mathis's Experience

124. Plaintiff Brandon Mathis was a customer of Defendant.

125. In order to obtain services from Defendant, Plaintiff was required to provide his PII to Defendant.

126. Plaintiff Mathis is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted

unencrypted sensitive PII over the internet or any other unsecured source.

127. At the time of the Data Breach, Defendant retained Plaintiffs' PII in its system.

128. Plaintiff Mathis received the Notice Letter, by U.S. mail, from Defendant, dated January 24, 2024. According to the Notice Letter, Plaintiffs' PII was improperly accessed and obtained by unauthorized third parties, including his name, Social Security number, address, loan number, and financial account information.

129. Upon receiving the Notice Letter from Defendant, Plaintiff Mathis has spent significant time dealing with the consequences of the Data Breach including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, communicating with his banks to dispute unauthorized charges to his credit and debit cards, replacing impacted credit and debit cards, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time 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.

130. Subsequent to the Data Breach, Plaintiff Mathis has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs 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; and (vii) the continued and certainly increased risk to his PII, 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 PII.

131. Plaintiff Mathis also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number, being in the hands of criminals.

132. The Data Breach has caused Plaintiff Mathis 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.

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

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

135. Plaintiff Mathis has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Nashira Williams's Experience

136. Plaintiff Nashira Williams is a customer of Defendant.

137. In order to obtain services from Defendant, Plaintiff Williams was required to provide her PII to Defendant.

138. Plaintiff Williams is very careful about sharing her sensitive PII. Plaintiff Williams stores any documents containing his PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

139. At the time of the Data Breach, Defendant retained Plaintiffs' PII in its system.

140. Plaintiff Williams received the Notice Letter, by U.S. mail, from Defendant, dated January 24, 2024. According to the Notice Letter, Plaintiffs' PII was improperly accessed and obtained by unauthorized third parties, including her name, Social Security number, address, loan number, and financial account information.

141. Upon receiving the Notice Letter from Defendant, Plaintiff Williams has spent significant time dealing with the consequences of the Data Breach including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time 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.

142. Subsequent to the Data Breach, Plaintiff Williams has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs 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; and (vii) the continued and certainly increased risk to his PII, 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 PII.

143. Plaintiff Williams also suffered actual injury in the form of experiencing an increase in spam texts and emails, which, upon information and belief, was caused by the Data

Breach.

144. Plaintiff Williams also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy, especially his Social Security number, being in the hands of criminals.

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

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

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

148. Plaintiff Williams has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Jaime Lee Mazzo's Experience

149. Plaintiff Jaime Lee Mazzo is a customer of Defendant.

150. In order to obtain services from Defendant, Plaintiff was required to provide his PII to Defendant.

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

152. At the time of the Data Breach, Defendant retained Plaintiffs' PII in its system.

153. Upon receiving information about the breach, Plaintiff Mazzo has spent significant time dealing with the consequences of the Data Breach including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time 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.

154. Subsequent to the Data Breach, Plaintiff Mazzo has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs 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; and (vii) the continued and certainly increased risk to his PII, 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 PII.

155. Plaintiff Mazzo suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number, being in the hands of criminals.

156. The Data Breach has caused Plaintiff Mazzo 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.

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

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

159. Plaintiff Mazzo has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Jeffrey Benson's Experience

160. Plaintiff Jeffrey Benson is a customer of Defendant.

161. In order to obtain services from Defendant, Plaintiff was required to provide his PII to Defendant.

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

163. At the time of the Data Breach, Defendant retained Plaintiffs' PII in its system.

164. Plaintiff Benson received the Notice Letter, by U.S. mail, from Defendant, dated January 24, 2024. According to the Notice Letter, Plaintiffs' PII was improperly accessed and obtained by unauthorized third parties, including his name, Social Security number, address, loan number, and financial account information.

165. Upon receiving the Notice Letter from Defendant, Plaintiff Benson has spent significant time dealing with the consequences of the Data Breach including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, communicating with

PayPal to dispute unauthorized charges to his account, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time 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.

166. Subsequent to the Data Breach, Plaintiff Benson has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs 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; and (vii) the continued and certainly increased risk to his PII, 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 PII.

167. Plaintiff Benson further suffered actual injury in the form of experiencing a series unauthorized Paypal transactions, which, upon information and belief, was caused by the Data Breach.

168. Plaintiff Benson also suffered actual injury in the form of experiencing an increase in spam texts and emails, which, upon information and belief, was caused by the Data Breach.

169. Plaintiff Benson also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number, being in the hands of criminals.

170. The Data Breach has caused Plaintiff Benson 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.

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

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

173. Plaintiff Benson has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Frank Canepa's Experience

174. Plaintiff Frank Canepa is a customer of Defendant.

175. In order to obtain services from Defendant, Plaintiff was required to provide his PII to Defendant.

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

177. At the time of the Data Breach, Defendant retained Plaintiffs' PII in its system.

178. Plaintiff Canepa received the Notice Letter, by U.S. mail, from Defendant, dated January 24, 2024. According to the Notice Letter, Plaintiffs' PII was improperly accessed and

obtained by unauthorized third parties, including his name, Social Security number, address, loan number, and financial account information.

179. Upon receiving the Notice Letter from Defendant, Plaintiff Canepa has spent significant time dealing with the consequences of the Data Breach including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, communicating with his banks to dispute unauthorized charges to his credit and debit cards, replacing impacted credit and debit cards, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time 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.

180. Subsequent to the Data Breach, Plaintiff Canepa has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs 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; and (vii) the continued and certainly increased risk to his PII, 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 PII.

181. Plaintiff Canepa further suffered actual injury in the form of experiencing five separate unauthorized charges, totaling approximately $2,500, to his Chase credit card, which, upon information and belief, was caused by the Data Breach.

182. Plaintiff Canepa also suffered actual injury in the form of experiencing an increase

in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

183. Plaintiff Canepa also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number, being in the hands of criminals.

184. The Data Breach has caused Plaintiff Canepa 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.

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

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

187. Plaintiff Canepa has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff William Ekola's Experience

188. Plaintiff William Ekola is a customer of Defendant.

189. In order to obtain services from Defendant, Plaintiff was required to provide his PII to Defendant.

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

191. At the time of the Data Breach, Defendant retained Plaintiffs' PII in its system.

192. Plaintiff Ekola received the Notice Letter, by U.S. mail, from Defendant, dated January 24, 2024. According to the Notice Letter, Plaintiffs' PII was improperly accessed and obtained by unauthorized third parties, including his name, Social Security number, address, loan number, and financial account information.

193. Upon receiving the Notice Letter from Defendant, Plaintiff Ekola has spent significant time dealing with the consequences of the Data Breach including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, communicating with his financial accounts to dispute unauthorized charges to his accounts, replacing impacted credit and debit cards, notifying credit bureaus of the fraud he experienced, and signing up for credit monitoring to monitor his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time 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.

194. Subsequent to the Data Breach, Plaintiff Ekola has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs 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; and (vii) the continued and certainly increased risk to his PII, 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 PII.

195. Plaintiff Ekola further suffered actual injury in the form of experiencing a charge totaling approximately $791 to his Discover account, in or about December 2023, which, upon information and belief, was caused by the Data Breach.

196. Plaintiff Ekola also suffered actual injury in the form of experiencing an increase in spam calls, which, upon information and belief, was caused by the Data Breach.

197. Plaintiff Ekola also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number, being in the hands of criminals.

198. The Data Breach has caused Plaintiff Ekola 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.

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

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

201. Plaintiff Ekola has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Joe Ward's Experience

202. Plaintiff Joe Ward is a customer of Defendant.

203. In order to obtain services from Defendant, Plaintiff was required to provide his PII to Defendant.

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

205. At the time of the Data Breach, Defendant retained Plaintiffs' PII in its system.

206. Plaintiff Ward received the Notice Letter, by U.S. mail, from Defendant, dated January 24, 2024. According to the Notice Letter, Plaintiffs' PII was improperly accessed and obtained by unauthorized third parties, including his name, Social Security number, address, loan number, and financial account information.

207. Upon receiving the Notice Letter from Defendant, Plaintiff Ward has spent significant time dealing with the consequences of the Data Breach including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, communicating with his banks to dispute unauthorized charges to his credit and debit cards, replacing impacted credit and debit cards, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time 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.

208. Subsequent to the Data Breach, Plaintiff Ward has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs 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; and (vii) the continued and certainly increased risk to his PII, 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 PII.

209. Plaintiff Ward further suffered actual injury in the form of experiencing a series of charges, totaling approximately $400, to his Wells Fargo debit card, in or about January 2024, which, upon information and belief, was caused by the Data Breach.

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

211. Plaintiff Ward also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number, being in the hands of criminals.

212. The Data Breach has caused Plaintiff Ward 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.

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

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

215. Plaintiff Ward has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Antonio Cole's Experience

216. Plaintiff Antonio Cole is a customer of Defendant.

217. In order to obtain services from Defendant, Plaintiff Cole was required to provide his PII to Defendant.

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

219. At the time of the Data Breach, Defendant retained Plaintiffs' PII in its system.

220. Plaintiff Cole received the Notice Letter, by U.S. mail, from Defendant, dated January 24, 2024. According to the Notice Letter, Plaintiffs' PII was improperly accessed and obtained by unauthorized third parties, including his name, Social Security number, address, loan number, and financial account information.

221. Upon receiving the Notice Letter from Defendant, Plaintiff Cole has spent significant time dealing with the consequences of the Data Breach including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, communicating with his banks to dispute unauthorized charges to his credit and debit cards, replacing impacted credit and debit cards, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time 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.

222. Subsequent to the Data Breach, Plaintiff Cole has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs 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; and (vii) the

continued and certainly increased risk to his PII, 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 PII.

223. Plaintiff Cole further suffered actual injury in the form of unauthorized charges on his debit/credit card, which, upon information Cole belief, was caused by the Data Breach. As a result of these unauthorized charges, Plaintiff Cole was forced to freeze and close his debit/credit card accounts.

224. Plaintiff Cole further suffered actual injury in the form of spending time to change his autopay information with several vendors.

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

226. Plaintiff Cole also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number, being in the hands of criminals.

227. The Data Breach has caused Plaintiff Cole 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.

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

229. As a result of the Data Breach, Plaintiff Cole is at a present risk and will continue

to be at increased risk of identity theft and fraud for years to come.

230. Plaintiff Cole has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Ramsey Coulter's Experience

231. Plaintiff Ramsey Coulter is a customer of Defendant.

232. In order to obtain services from Defendant, Plaintiff Coulter was required to provide his PII to Defendant.

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

234. At the time of the Data Breach, Defendant retained Plaintiffs' PII in its system.

235. Plaintiff Coulter received the Notice Letter, by U.S. mail, from Defendant, dated January 24, 2024. According to the Notice Letter, Plaintiffs' PII was improperly accessed and obtained by unauthorized third parties, including his name, Social Security number, address, loan number, and financial account information.

236. Upon receiving the Notice Letter from Defendant, Plaintiff Coulter has spent significant time dealing with the consequences of the Data Breach including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time 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.

237. Subsequent to the Data Breach, Plaintiff Coulter suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs 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; and (vii) the continued and certainly increased risk to his PII, 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 PII.

238. Plaintiff Coulter further suffered actual injury in the form of a flood of spam telephone calls from unknown persons since the Data Breach. Plaintiff Coulter's personal bank account was also hacked. As such, Plaintiff has already been subjected to violations of his privacy, fraud, and identity theft, and has been exposed to a heightened and imminent risk of fraud and identity theft.

239. Plaintiff Coulter must now and in the future spend time closely monitoring his bank account, credit reports, phone lines, and online accounts to guard against identity theft.

240. Plaintiff has also incurred out-of-pocket costs for, among other things, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

241. Plaintiff Coulter also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss

of his privacy, especially his Social Security number, being in the hands of criminals.

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

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

244. Plaintiff Coulter has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

245. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and 23(b)(3).

246. Plaintiffs bring this action on behalf of themselves and all members of the following Class of similarly situated persons:

> **All persons whose PII was compromised in the Data Breach first announced by Defendant Planet Home Lending, LLC in January 2024.**

247. Excluded from the Class are Defendant and their affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

248. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

249. The members of the Class are so numerous that joinder of each of the Class Members in a single proceeding would be impracticable. According to reports, Defendant's breach impacted approximately 200,000 people.

250. Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' PII from unauthorized access and disclosure;

b. Whether Defendant had a duty not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' PII;

d. Whether an implied contract existed between Class Members and Defendant, providing that Defendant would implement and maintain reasonable security measures to protect and secure Class Members' PII from unauthorized access and disclosure;

e. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

f. Whether Defendant breached its duties to protect Plaintiffs' and Class Members' PII; and

g. Whether Plaintiffs and Class Members are entitled to damages and the measure of such damages and relief.

251. Typicality: Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other member of the Class.

252. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant 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. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

253. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

254. 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 corporations, like Defendant. 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.

255. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant 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 Plaintiffs were 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.

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

257. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

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

259. Further, Defendant has 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.

COUNT I
NEGLIGENCE

260. Plaintiffs reallege and incorporates by reference paragraphs 1-132 as if fully set forth herein.

261. Defendant requires its customers, including Plaintiffs and Class Members, to submit non-public PII in the ordinary course of providing its services.

262. Defendant gathered and stored the PII of Plaintiffs and Class Members as part of its business of soliciting its services to its customers, which solicitations and services affect commerce.

263. Plaintiffs and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

264. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

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

266. Defendant 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.

267. Defendant's duty to use reasonable security measures under which they were required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

268. Defendant owed a duty of care to Plaintiffs 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 PII.

269. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential PII, a necessary part of being customers with Defendant.

270. Defendant's 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 Defendant is bound by industry standards to protect confidential PII.

271. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

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

273. Moreover, Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiffs and the Class within Defendant's 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 Plaintiffs and the Class to take

steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

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

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

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

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII;

e. Failing to detect in a timely manner that Class Members' PII had been compromised;

f. Failing to remove former customers' PII it was no longer required to retain pursuant to regulations,

g. 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; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

275. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in

detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

276. Plaintiffs and the Class are within the class of persons that the FTC Act and other standards were intended to protect.

277. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and standards were intended to guard against.

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

279. 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 Plaintiffs and the Class.

280. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

281. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII 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 in the lending industry.

282. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

283. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical

importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

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

285. Plaintiffs and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

286. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

287. Defendant's duty extended to protecting Plaintiffs 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.

288. Defendant has admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

289. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

290. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in

safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

291. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs 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; and (vii) the continued and certainly increased risk to their PII, 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 PII.

292. As a direct and proximate result of Defendant's negligence, Plaintiffs 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.

293. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain 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 PII in its continued possession.

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

295. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiffs and Class Members in an unsafe and insecure manner.

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

COUNT II
NEGLIGENCE *PER SE*

297. Plaintiffs reallege and incorporates by reference paragraphs 1-132 as if fully set forth herein.

298. 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 Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

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

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

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

302. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) were 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 Plaintiffs and Class Members.

303. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

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

305. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs 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; and (vii) the continued and certainly increased risk to their PII, 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 PII.

306. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs 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.

307. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain 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 PII in its continued possession.

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

309. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiffs and Class Members in an unsafe and insecure manner.

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

COUNT III
BREACH OF IMPLIED CONTRACT

311. Plaintiffs reallege and incorporates by reference paragraphs 1-132 as if fully set forth herein.

312. Plaintiffs and Class Members were required to provide their PII to Defendant as a condition of receiving products and/or services from Defendant.

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

314. Implicit in the agreement between Plaintiffs and Class Members and the Defendant 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 Plaintiffs 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 Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

315. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

316. Defendant solicited, offered, and invited Plaintiffs and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

317. In accepting the PII of Plaintiffs and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

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

319. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' PII would remain protected.

320. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

321. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

322. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

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

324. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

325. Defendant breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

326. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

327. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

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

COUNT IV
UNJUST ENRICHMENT

329. Plaintiffs reallege and incorporates by reference paragraphs 1-132 as if fully set forth herein.

330. Plaintiffs bring this count in the alternative to the breach of implied contract count above.

331. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for products and/or services from Defendant and/or its agents and in so doing also provided Defendant with their PII. In exchange, Plaintiffs and Class Members should have received from Defendant the products and/or services that were the subject of the transaction and should have had their PII protected with adequate data security.

332. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form their PII as well as payments made on their behalf as a necessary part of obtaining products and/or services. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

333. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of

Plaintiffs and Class Members.

334. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

335. Defendant, however, failed to secure Plaintiffs' and Class Members' PII and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

336. Defendant would not be able to carry out an essential function of its regular business without the PII of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

337. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

338. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their PII, they would not have allowed their PII to be provided to Defendant.

339. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' 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 Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a

direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their PII.

340. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

341. Plaintiffs and Class Members have no adequate remedy at law.

342. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs 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; and (vii) the continued and certainly increased risk to their PII, 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 PII.

343. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

344. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received

from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

COUNT V
DECLARATORY JUDGMENT

345. Plaintiffs reallege and incorporates by reference paragraphs 1-132 as if fully set forth herein.

346. 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 that are tortious and violate the terms of the federal statutes described in this Complaint.

347. Defendant owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

348. Defendant still possesses Private Information regarding Plaintiffs and Class Members.

349. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs continues to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

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

a. Defendant owes a legal duty to secure its customers' Private Information and to timely notify customers of a data breach under the common law and Section 5 of the FTCA;

b. Defendant's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect customers' Private Information; and

c. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure customers' Private Information.

351. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect customers' Private Information, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

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

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its users about the threats they face with regard to the security of their Private Information, as well as the steps PHL's customers should take to protect themselves.

352. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach of Defendant's computer system. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

353. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

354. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach of

Defendants computer system, thus preventing future injury to Plaintiffs and other customers whose Private Information would be further compromised.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in his favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing yet another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: April 1, 2024

By: */s/ Oren Faircloth*

Oren Faircloth, CT Bar #438105
Mason A. Barney*
Tyler J. Bean*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Telephone: (212) 532-1091
Email: ofaircloth@sirillp.com
Email: mbarney@sirillp.com
Email: tbean@sirillp.com

Daniel Srourian, Esq.*
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd., Suite 1710
Los Angeles, California 90010
Telephone: (213) 474-3800
Facsimile: (213) 471-4160
Email: daniel@slfla.com

Gary E. Mason*
Danielle L. Perry*
Lisa A. White*
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
Email: gmason@masonllp.com
Email: dperry@masonllp.com
Email: lwhite@masonllp.com

Jeff Ostrow*
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-332-4200
Email: ostrow@kolawyers.com

Raina Borrelli*
TURKE & STRAUSS LLP

613 Williamson St., Suite 201
Madison, Wisconsin 53703
Telephone: 608-237-1775
Facsimile: 608-509-4423
Email: raina@turkestrauss.com

Mariya Weekes
Florida Bar No. 56299
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
201 Sevilla Avenue, 2nd Floor
Coral Gables, FL 33134
Tel: (786) 879-8200
Fax: (786) 879-7520
Email: mweekes@milberg.com

Interim Class Counsel

**Pro Hac Vice Forthcoming*