UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

BRANDON MATHIS, on behalf of himself and all others similarly situated, Plaintiff, v. **PLANET HOME LENDING, LLC,** Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Brandon Mathis ("Plaintiff"), individually and on behalf of all similarly situated persons, alleges the following against Planet Home Lending, LLC ("PHL" or "Defendant") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by his counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against PHL for its failure to properly secure and safeguard Plaintiff's and other similarly situated PHL customers' name, address, Social Security number, loan number, and financial account number (the "Private Information") from hackers.

2. PHL, based in Meriden, Connecticut is a full-service mortgage company that serves hundreds of thousands of customers nationwide.

3. On or about January 25, 2024, PHL filed official notice of a hacking incident with the Office of the Maine Attorney General.[1]

4. On or around the same time, PHL also sent out data breach letters (the "Notice") to individuals whose information was compromised as a result of the hacking incident.

5. Based on the Notice sent to Plaintiff and "Class Members" (defined below), PHL detected unusual activity on some of its computer systems on or around November 15, 2023. In response, the company launched a forensic investigation that revealed that the cybercriminal organization, LockBit, had gained unauthorized access to certain company files on November 15, 2023 (the "Data Breach").

6. Plaintiff and Class Members were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, customers' Social Security number, loan number, and financial account number that PHL collected and maintained.

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/5f9aa393-9c7a-49e0-855f-5e36adfb9e6c.shtml (last visited Jan. 31, 2024).

9. There has been no assurance offered by PHL that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

10. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiff brings this class action lawsuit to address PHL's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

12. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to PHL, and thus PHL was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, PHL and its employees failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information.

14. Plaintiff's and Class Members' identities are now at risk because of PHL's negligent conduct as the Private Information that PHL collected and maintained is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Accordingly, Plaintiff, on behalf of himself and the Class, asserts claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, and declaratory judgment.

II. PARTIES

17. Plaintiff Brandon Mathis is, and at all times mentioned herein was, an individual citizen of the State of Florida.

18. Defendant, Planet Home Lending, LLC, is a home loan service company incorporated in Delaware with its principal place of business at 321 Research Parkway, Suite 303, Meriden, Connecticut 06450.

III. JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from PHL. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has jurisdiction over PHL because PHL operates in and/or is incorporated in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and PHL has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. PHL's Business and Collection of Plaintiff's and Class Members' Private Information

22. PHL is a full-service mortgage company. Founded in 2007, PHL offers financial services for residential homeowners including mortgage loan services, veterans affairs loan services, and home refinancing. PHL serves more than 199,873 customers in numerous states, employs more than 1,000 people and generates approximately $490 million in annual revenue.

23. As a condition of receiving financial services, PHL requires that its customers entrust it with highly sensitive personal information. In the ordinary course of receiving service from PHL, Plaintiff and Class Members were required to provide their Private Information to Defendant.

24. PHL uses this information, *inter alia*, for advertising and marketing.

25. In its Consumer Privacy Notice, PHL promises its customers that it will "protect the privacy of our clients' personal information and their customers' data" and that it "will not sell, share, or rent this information to others in ways different from what is disclosed in this Privacy Statement."[2]

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

27. Plaintiff and Class Members relied on PHL to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendant ultimately failed to do.

[2] *See* https://planethomelending.com/privacy-policy/ (last visited Jan. 31, 2024).

B. The Data Breach and PHL's Inadequate Notice to Plaintiff and Class Members

28. According to Defendant's Notice, which Plaintiff received in late January of 2024, PHL learned of unauthorized access to its computer systems on November 15, 2023, with such unauthorized access having been carried out by renowned threat actor, LockBit.

29. Through the Data Breach, LockBit accessed a cache of highly sensitive Private Information, including customers' "name, address, Social Security number, loan number, and financial account number."

30. More than two months after PHL learned that the Class's Private Information was first accessed by LockBit, PHL finally began to notify customers that its investigation determined that their Private Information was impacted.

31. PHL delivered Data Breach Notification Letters to Plaintiff and Class Members, alerting them that their highly sensitive Private Information had been exposed in a "data breach."

32. The notice letter then listed generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Other than providing two years of crediting monitoring that Plaintiff and Class Members would have to affirmatively sign up for and a call center number that victims could contact with questions, PHL offered no other substantive steps to help victims like Plaintiff and Class Members to protect themselves. On information and belief, PHL sent a similar generic letter to all individuals affected by the Data Breach.

33. PHL had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

34. Plaintiff and Class Members provided their Private Information to PHL with the reasonable expectation and mutual understanding that PHL would comply with its obligations to

keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

35. PHL's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

36. PHL knew or should have known that its electronic records would be targeted by cybercriminals.

C. PHL Failed to Comply with FTC Guidelines

37. 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. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

38. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The 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. 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 into 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.

39. The FTC further recommends that companies not maintain personally identifiable information ("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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

40. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

41. As evidenced by the Data Breach, PHL failed to properly implement basic data security practices. PHL's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

42. PHL was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. PHL Failed to Comply with Industry Standards

43. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

44. Some industry best practices that should be implemented by businesses like PHL include but are not limited to educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor

authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

45. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

46. 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.

47. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

E. PHL Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

48. In addition to its obligations under federal laws, PHL owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. PHL owed a duty to Plaintiff and Class Members to provide reasonable security, including complying with industry standards and

requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

49. PHL breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. PHL's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its customers Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

50. PHL negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

51. Had PHL remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field,

it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

52. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with PHL.

F. PHL Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft

53. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[3] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

54. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

[3] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Jan. 31, 2024).

55. Because a person's identity is akin to a puzzle, 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 to otherwise harass or track the victim. 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 individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

56. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

57. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

58. One such example of this is the development of "Fullz" packages.

59. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach 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. These dossiers are known as "Fullz" packages.

60. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can 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. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen Private Information are being misused, and that such misuse is fairly traceable to the Data Breach.

61. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[4] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

62. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security

[4] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Jan. 31, 2024).

number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

63. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

64. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[5] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry.

65. The PII of consumers 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. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[6] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[7]

---

[5] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military (last visited on Jan. 31, 2024).

[6] *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 on Jan. 31, 2024).

[7] *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 on Jan. 31, 2024).

66. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[8]

67. The Dark Web Price Index of 2022, published by PrivacyAffairs[9] shows how valuable just email addresses alone can be, even when not associated with a financial account:

Email Database Dumps	**Avg. Price USD (2022)**
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

68. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

69. Likewise, the value of PII is increasingly evident in our digital economy. Many companies including PHL collect PII for purposes of data analytics, advertising, and marketing.

[8] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on Jan. 31, 2024).

[9] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited on Jan. 31, 2024).

These companies, collect it to better target customers, and shares it with third parties for similar purposes.[10]

70. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[11]

71. Consumers also recognize the value of their personal information and offer it in exchange for goods and services or sell it through legitimate data brokers. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

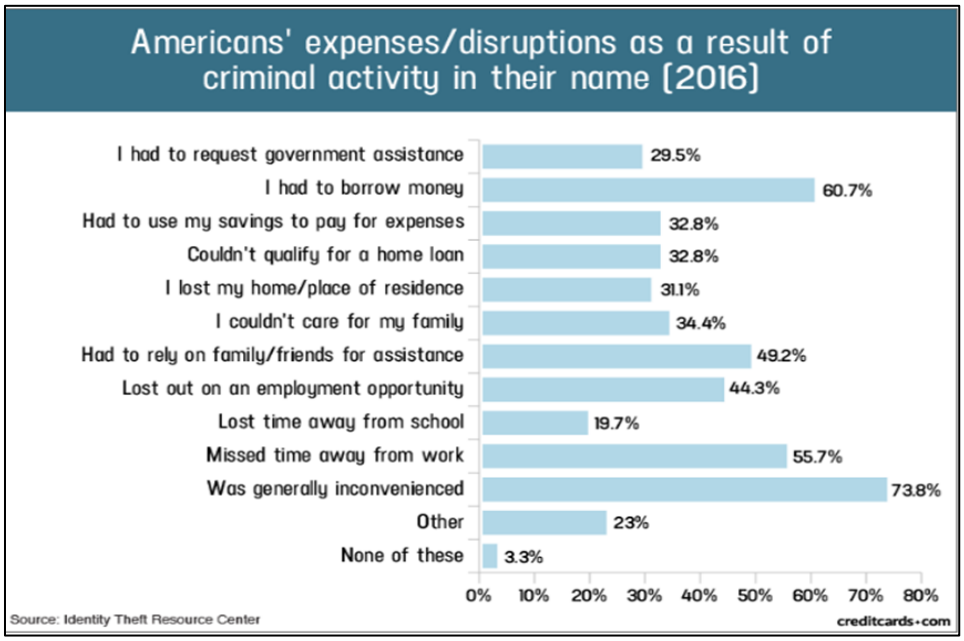
72. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

73. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiff's PII impairs their ability to participate in the economic marketplace.

[10] *See* https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on Jan. 31, 2024).

[11] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

74. A study by the Identity Theft Resource Center[12] shows the multitude of harms caused by fraudulent use of PII:



75. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[13]

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

[12] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited Jan. 31, 2024).

[13] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Jan. 31, 2024).

76. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

77. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

G. Plaintiff's and Class Members' Damages

Plaintiff Brandon Mathis' Experience

78. When Plaintiff Mathis first became a customer, Defendant required Plaintiff Mathis provide it with substantial amounts of his PII.

79. On or about January 24, 2024, Plaintiff Mathis received a letter entitled "Notice of Data Breach" which told him that his Private Information had been impacted during the Data Breach. The notice letter informed him that the Private Information compromised included his "name, address, Social Security number, loan number, and financial account number."

80. The notice letter offered Plaintiff Mathis only two years of credit monitoring services. Two years of credit monitoring is not sufficient given that Plaintiff Mathis will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of his Private Information.

81. Plaintiff Mathis suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

82. Plaintiff Mathis would not have provided his Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its customers' personal information from theft, and that those systems were subject to a data breach.

83. Plaintiff Mathis suffered actual injury in the form of having his Private Information compromised and/or stolen as a result of the Data Breach.

84. Plaintiff Mathis suffered actual injury in the form of damages to and diminution in the value of his personal and financial information – a form of intangible property that Plaintiff Mathis entrusted to Defendant for the purpose of receiving financial services from Defendant and which was compromised in, and as a result of, the Data Breach.

85. Plaintiff Mathis suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

86. Plaintiff Mathis has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

87. As a result of the Data Breach, Plaintiff Mathis made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options he will now need to use. Plaintiff Mathis has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

88. As a result of the Data Breach, Plaintiff Mathis has suffered anxiety as a result of the release of his Private Information to cybercriminals, which Private Information he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of committing cyber and other crimes against him. Plaintiff Mathis is very concerned about this

increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on his life.

89. Plaintiff Mathis also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Mathis; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

90. 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 the many harms caused by the Data Breach.

91. In sum, Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

92. Plaintiff and Class Members entrusted their Private Information to Defendant in order to receive Defendant's services.

93. Plaintiff's Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

94. As a direct and proximate result of PHL's actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

95. Further, as a direct and proximate result of PHL's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

96. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

97. The Private Information maintained and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

98. Plaintiff and Class Members also lost the benefit of the bargain they made with PHL. Plaintiff and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiff and Class Members paid to PHL was intended to be used by PHL to fund adequate security of PHL's system and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class did not receive what they paid for.

99. Additionally, as a direct and proximate result of PHL's conduct, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

100. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

101. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[14] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[15]

102. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

103. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. The contractual bargain entered into between Plaintiff and PHL included Defendant's

[14] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on Jan. 31, 2024).

[15] *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Jan. 31, 2024).

contractual obligation to provide adequate data security, which Defendant failed to provide. Thus, Plaintiff and Class Members did not get what they bargained for.

104. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Addressing their inability to withdraw funds linked to compromised accounts;

d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

e. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

f. Contacting financial institutions and closing or modifying financial accounts;

g. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

h. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

i. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

105. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of PHL, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

106. As a direct and proximate result of PHL's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

107. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

108. Specifically, Plaintiff proposes the following Nationwide Class, (referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States who had Private Information accessed and/ or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

109. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

110. Plaintiff reserves the right to modify or amend the definition of the proposed Nationwide Class, and to add subclasses before the Court determines whether certification is appropriate.

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

112. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of almost 200,000 current and former customers of PHL whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through PHL's records, Class Members' records, publication notice, self-identification, and other means.

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

a. Whether PHL engaged in the conduct alleged herein;

b. When PHL learned of the Data Breach;

c. Whether PHL's response to the Data Breach was adequate;

d. Whether PHL unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

e. Whether PHL failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether PHL's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether PHL's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether PHL owed a duty to Class Members to safeguard their Private Information;

i. Whether PHL breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether PHL knew or should have known that its data security systems and monitoring processes were deficient;

l. What damages Plaintiff and Class Members suffered as a result of PHL's misconduct;

m. Whether PHL's conduct was negligent;

n. Whether PHL's conduct was *per se* negligent;

o. Whether PHL was unjustly enriched;

p. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

q. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

114. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

115. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

116. Predominance. PHL has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from PHL's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

117. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for PHL. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

118. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). PHL has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

119. Finally, all members of the proposed Class are readily ascertainable. PHL has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by PHL.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class)

120. Plaintiff restates and realleges all of the allegations stated above and hereafter as if fully set forth herein.

121. PHL knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

122. PHL knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. PHL was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

123. PHL owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. PHL's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession; and

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the FTCA.

124. PHL's duty to employ reasonable data security measures arose, in part, 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.

125. PHL's duty also arose because Defendant was bound by industry standards to protect its customers' confidential Private Information.

126. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and PHL owed them a duty of care to not subject them to an unreasonable risk of harm.

127. PHL, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within PHL's possession.

128. PHL, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

129. PHL breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. 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' Private Information;

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

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

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

e. Failing to comply with the FTCA;

130. PHL had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust PHL with their Private Information was predicated on the understanding that PHL would take adequate security precautions. Moreover, only PHL had the ability to protect its systems (and the Private Information that it stored on them) from attack.

131. PHL's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

132. PHL's breach of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

133. As a result of PHL's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

134. PHL also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

135. As a direct and proximate result of PHL's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

136. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

137. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

138. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring PHL to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Nationwide Class)

139. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

140. Pursuant to Section 5 of the FTCA, PHL had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

141. PHL breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

142. Plaintiff and Class Members are within the class of persons that the FTCA is intended to protect.

143. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of PHL's duty in this regard.

144. PHL violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

145. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to PHL's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

146. PHL's violations of the FTCA constitute negligence *per se*.

147. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to PHL's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

148. As a direct and proximate result of PHL's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

149. PHL breached its duties to Plaintiff and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

150. As a direct and proximate result of PHL's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

151. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring PHL to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class)

152. Plaintiff restates and realleges the allegations in paragraphs as if fully set forth herein.

153. This Count is pleaded in the alternative to Count III above.

154. PHL provides mortgage loan services to Plaintiff and Class Members. Plaintiff and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiff and Class Members paying for services from Defendant.

155. Through Defendant's sale of services, it knew or should have known that it must protect Plaintiff's and Class Members' confidential Private Information in accordance with PHL's policies, practices, and applicable law.

156. As consideration, Plaintiff and Class Members paid money to PHL and turned over valuable Private Information to PHL. Accordingly, Plaintiff and Class Members bargained with PHL to securely maintain and store their Private Information.

157. PHL accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members.

158. In delivering their Private Information to PHL and paying for services, Plaintiff and Class Members intended and understood that PHL would adequately safeguard the Private Information as part of that service.

159. Defendant's implied promises to Plaintiff and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

160. Plaintiff and Class Members would not have entrusted their Private Information to PHL in the absence of such an implied contract.

161. Had PHL disclosed to Plaintiff and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and Class Members would not have provided their Private Information to PHL.

162. PHL recognized that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

163. PHL violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Private Information.

164. Plaintiff and Class Members have been damaged by PHL's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class)

165. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

166. This Count is pleaded in the alternative to Count III above.

167. Plaintiff and Class Members conferred a benefit on PHL by turning over their Private Information to Defendant and by paying for services that should have included cybersecurity protection to protect their Private Information. Plaintiff and Class Members did not receive such protection.

168. Upon information and belief, PHL funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiff and Class Members.

169. As such, a portion of the payments made by Plaintiff and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to PHL.

170. PHL has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiff and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

171. PHL knew that Plaintiff and Class Members conferred a benefit upon it, which PHL accepted. PHL profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiff's and Class Members' Private Information and prevented the Data Breach.

172. If Plaintiff and Class Members had known that PHL had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

173. Due to PHL's conduct alleged herein, it would be unjust and inequitable under the circumstances for PHL to be permitted to retain the benefit of its wrongful conduct.

174. As a direct and proximate result of PHL's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in PHL's possession and is subject to further unauthorized disclosures so long as PHL fails to undertake appropriate and

adequate measures to protect Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

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

COUNT V
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Nationwide Class)

177. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

178. 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.

179. PHL owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

180. PHL still possesses Private Information regarding Plaintiff and Class Members.

181. Plaintiff alleges that PHL's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his Private Information and the risk remains that further compromises of his Private Information will occur in the future.

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

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

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

a. Order PHL to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, PHL 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 PHL'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.

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

185. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to PHL if an injunction is issued. Plaintiff 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 PHL's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and PHL has a pre-existing legal obligation to employ such measures.

186. 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 at PHL, thus preventing future injury to Plaintiff and other customers whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing PHL to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring PHL to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: January 31, 2024.

Respectfully submitted,

/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
Tel: (212) 532-1091
E: ofaircloth@sirillp.com
E: mbarney@sirillp.com
E: tbean@sirillp.com

Attorneys for Plaintiff and the Putative Class

**Pro hac vice application forthcoming*

ClassAction.org
