UNITED STATES DISTRICT COURT
DISTRICT OF MIDDLE DISTRICT OF FLORIDA
JACKSONVILLE DIVISION

DANIEL HERNANDEZ and NAMUUN BAT, individually and on behalf of all others similarly situated, Plaintiffs, v. FIDELITY NATIONAL FINANCIAL, INC. and LOANCARE, LLC, Defendants.	Case No.: **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Daniel Hernandez and Namuun Bat ("Plaintiffs") bring this class action against Defendants Fidelity National Financial Inc. ("FNF") and LoanCare, LLC ("LoanCare") (collectively, "Defendants") on behalf of themselves and all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard personally identifiable information ("PII" or "Private Information")[1] including (but not limited to), Plaintiffs and Class Members' names,

[1] Personally identifiable information generally incorporates information that can be used to

addresses, Social Security numbers, and loan numbers.

2. FNF is the leading provider of title insurance and settlement services to the real estate and mortgage industries.[2] FNF's "various mortgage and real estate service companies provide services that complement [FNF's] title insurance business."[3]

3. LoanCare is a direct subsidiary of FNF. LoanCare specializes in servicing mortgage loans for banks, credit unions, and independent mortgage companies.[4] LoanCare serves nearly 1.5 million customers each year.[5] LoanCare allowed FNF access and control over its consumers' highly sensitive PII.

4. To provide their services, and in the ordinary course of Defendants' business, Defendants acquire, possess, maintain, analyze, and otherwise utilize Plaintiffs' and Class Members' Private Information.

5. Plaintiffs seek to hold Defendants responsible for the harms they caused, and will continue to cause, the approximately 1,316,938 individuals including Plaintiffs and

---

distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

[2] https://fnf.com/.

[3] *Id.*

[4] https://myloancare.com/web/about-us.

[5] *Id.*

other similarly situated persons[6] in the massive and preventable cyberattack that occurred, due to Defendants' negligence, by which cybercriminals from the ransomware group known as Alphv infiltrated Defendants' inadequately protected network and accessed and exfiltrated highly sensitive, unencrypted PII belonging to Plaintiffs and Class Members. (the "Data Breach").

6. Plaintiffs further seek to hold Defendants responsible for their negligence and dereliction of duties in not maintaining adequate security measures, consistent with industry standards, to protect Plaintiffs PII.

7. On or about December 13, 2023, Defendants notified state Attorneys General and many Class Members about the widespread Data Breach (the "Notice Letter").[7]

8. According to the Notice Letter, on or about November 19, 2023, LoanCare became aware of unauthorized access to certain systems within FNF's computer network, indicating a data breach. A subsequent investigation confirmed that unauthorized cybercriminals accessed Defendants' inadequately secured network and thereby "exfiltrated data from certain FNF systems." Defendants' investigation further determined that Plaintiffs and Class Members' PII were among the data "obtained by the unauthorized third party."[8]

---

[6] https://apps.web.maine.gov/online/aeviewer/ME/40/25bd9abc-608b-4a8a-8f35-ba5413b9399f.shtml.

[7] *See id.* (Sample Notice Letter available on the Office of the Maine Attorney General website).

[8] *Id.*

9. The Notice Letter provides no further information regarding the Data Breach and only recommends how victims can place a fraud alert or credit freeze on their account and how to sign up for the limited and abbreviated identity monitoring services Defendants offered in response to the Data Breach. The Notice Letter does not explain how the Data Breach occurred, what steps Defendants took following the Data Breach, whether Defendants made any changes to its data security, or most importantly, whether Plaintiffs' and Class Members' PII remains in the possession of criminals.

10. Further, the Notice Letter failed to advise Plaintiffs and Class Members that their information had been stolen by a notorious and aggressive Alphv, also known as BlackCat, ransomware gang. Instead, this information came to light only as a result of posts by Alphv/BlackCat, which were then reported by various journalists, wherein the gang took credit for the Data Breach.[9]

11. On information and belief, Alphv/BlackCat is anticipated to release all stolen information onto the dark web for access, sale, and download following the deadline of the ransom demand to Defendants.[10]

12. By acquiring, utilizing, and benefiting from Plaintiffs' and Class Members' PII for its business purposes, Defendants owed or otherwise assumed common law, contractual, and statutory duties that extended to Plaintiffs and Class Members. These

[9] *See, e.g.,* https://www.securityweek.com/loancare-notifying-1-3-million-of-data-breach-following-cyberattack-on-parent-company/; https://www.scmagazine.com/brief/over-1-3m-confirmed-by-loancare-to-be-hit-by-cyberattack.

[10] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a.

duties required Defendants to design and implement adequate data security systems to protect Plaintiffs' and Class Members' PII in its possession and to keep Plaintiffs' and Class Members' PII confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

13. Defendants breached these duties by failing to implement adequate data security measures and protocols to properly safeguard and protect Plaintiffs' and Class Members' PII from a foreseeable cyberattack on its systems that resulted in the unauthorized access and theft of Plaintiffs' and Class Members' PII.

14. Currently, the full extent of the types of PII, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendants, its agents, counsel, and forensic security vendors at this phase of the litigation.

15. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement 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 Plaintiffs' and Class Members' PII was compromised through disclosure to an unknown and unauthorized criminal third party.

16. Upon information and belief, Defendants breached their duties and obligations in one or more of the following ways: (1) failing to design or being negligent

in the design, implementation, monitor, and maintaining reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiffs and Class Members of Defendants' inadequate data security practices; (6) failing to encrypt or adequately encrypt the PII; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to prevent this type of attack; and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

17. Based on the type of sophisticated and targeted criminal activity, the type of PII involved, and that the PII was accessed and exfiltrated by an unauthorized criminal ransomware group, it is clear that the unauthorized cybercriminals were able to successfully target Plaintiffs' and Class Members' PII, infiltrate and gain access to Defendants' network, and exfiltrate Plaintiffs' and Class Members' PII, for the purposes of utilizing or selling the PII for use in future fraud and identity theft related cases.

18. As a result of Defendants' failures and the Data Breach, Plaintiffs' and Class Members' identities are now at a current, substantial, imminent and ongoing risk of identity theft and they shall remain at risk for the rest of their lives.

19. As Defendants instructed, advised, and warned in its Notice Letter discussed below, Plaintiffs and Class Members must now closely monitor their financial accounts to

guard against future identity theft and fraud. Plaintiffs and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will include into the future: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

20. Plaintiffs and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time heeding Defendants' warnings and following its instructions in the Notice Letter; (g) deprivation of value of their PII; (h) invasions of their privacy; and (i) the continued risk to their PII, which remains in the possession of Defendants, and is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect it.

21. Plaintiffs bring this action on behalf of all persons whose PII was compromised due to Defendants' failure to adequately protect Plaintiffs' and Class Members' PII. Accordingly, Plaintiffs seek redress for Defendants' unlawful conduct and assert claims on behalf of the Class.

PARTIES

Plaintiffs

22. Plaintiff Daniel Hernandez ("Hernandez") is a natural person and citizen of Texas. He resides in Groves, Texas where he intends to remain.

23. Plaintiff Namuun Bat ("Bat") is a natural person and citizen of California. She resides in Folsom, California where she intends to remain.

Defendants

24. Defendant Fidelity National Financial, Inc. is a Delaware corporation with its principal place of business at 601 Riverside Ave., Building 5, Jacksonville, Florida.

25. Defendant LoanCare, LLC is a Virginia limited liability company whose principal place of business is at 3673 Sentara Way, Virginia Beach, Virginia, and it is authorized to transact business in Florida. Upon information and belief, the sole member of LoanCare, LLC is Defendant FNF.

JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and various members of the class, including Plaintiffs Deschamps and Washington, are citizens of a state different from Defendants.

27. This Court has general personal jurisdiction Defendants because one Defendant, FNF, maintains its principal place of business is in this District, and both

Defendants have sufficient minimum contacts in this District and have intentionally availed themselves of this jurisdiction by marketing and selling services, and by accepting and processing payments for those services within this State and District.

28. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant FNF has a principal place of business is in this District, and because a substantial part of the events that gave rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Background

29. Defendants are title and mortgage servicing companies.

30. In the ordinary course of its business, Defendants collect and maintain the PII of its current and former customers. Additionally, Defendants may receive PII from other organizations including Plaintiffs' and Class Members' mortgage lenders.

31. Because of the highly sensitive and personal nature of the information Defendants acquire and store, Defendants, upon information and belief, promise to, among other things to keep protected health information private; comply with industry standards related to data security and PII, inform consumers of its legal duties and comply with all federal and state laws protecting consumer PII; only use and release PII for reasons that are required for legitimate business purposes or to comply with legal obligations, and, provide adequate notice to individuals if their PII is disclosed without authorization.

32. Indeed, the Privacy Policy posted on FNF's website reassures: "[FNF] and its majority-owned subsidiary companies respect and are committed to protecting your privacy."[11]

33. At every step, Defendants hold onto sensitive PII and have a duty to protect that PII from unauthorized access.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure.

35. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

36. Plaintiffs and Class Members relied on Defendants to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use their PII solely for proper business services and purposes, and to prevent the unauthorized disclosure of their PII.

The Cyberattack and Data Breach

37. On or about December 13, 2023, Defendants notified state Attorneys General and many Class Members about the widespread Data Breach (the "Notice Letter").[12]

[11] https://fnf.com/privacy-notice.

[12] *See id.* (Sample Notice Letter available on the Office of the Maine Attorney General website).

38. According to the Notice Letter, on or about November 19, 2023, LoanCare became aware of unauthorized access to certain systems within FNF's computer network, indicating a data breach. A subsequent investigation confirmed that unauthorized cybercriminals accessed Defendants' inadequately secured network and thereby "exfiltrated data from certain FNF systems." Defendants' investigation further determined that Plaintiffs and Class Members' PII were among the data "obtained by the unauthorized third party."[13]

39. The Notice Letter provides no further information regarding the Data Breach and only recommends how victims can place a fraud alert or credit freeze on their account and how to sign up for the limited and abbreviated identity monitoring services Defendants offered in response to the Data Breach. The Notice Letter does not explain how the Data Breach occurred, what steps Defendants took following the Data Breach, whether Defendants made any changes to its data security, or most importantly, whether Plaintiffs' and Class Members' PII remains in the possession of criminals.

40. Further, the Notice Letter failed to advise Plaintiffs and Class Members that their information had been stolen by a notorious and aggressive Alphv, also known as BlackCat, ransomware gang. Instead, this information came to light only as a result of posts by Alphv/BlackCat, which were then reported by various journalists, wherein the gang took credit for the Data Breach.[14]

---

[13] *Id.*

[14] *See, e.g.,* https://www.securityweek.com/loancare-notifying-1-3-million-of-data-

41. Upon information and belief, Plaintiffs' and Class Members' PII was exfiltrated and stolen in the Data Breach.

42. Based on Alphv/BlackCat's history of releasing PII on the dark web, it is near certain that Plaintiffs' and the Class's Private Information has been released on the dark web or will be released on the dark web soon.[15]

43. Defendants had obligations created by contract, industry standards, common law, and their own promises and representations to keep Plaintiffs' and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

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

45. Through its Notice Letter, Defendants also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to take steps to mitigate their risk of identity theft, such as reviewing financial accounts, and reviewing credit reports for possible fraud.

46. Defendants has offered abbreviated, non-automatic credit monitoring services to victims thereby identifying the harm posed to Plaintiffs and Class Members as a result of the Data Breach, which does not adequately address the lifelong harm that

---

breach-following-cyberattack-on-parent-company/; https://www.scmagazine.com/brief/over-1-3m-confirmed-by-loancare-to-be-hit-by-cyberattack.

[15] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a.

victims face following the Data Breach. Indeed, the Data Breach involves PII that cannot be changed, such as Social Security numbers.

47. The Notice Letters sent to Plaintiffs and Class Members stated PII, including names, addresses, and Social Security numbers, and loan numbers, was accessed and exfiltrated in the Data Breach.

48. As a result of the Data Breach, Plaintiffs and more than 1.3 Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

49. This PII was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and Class Members.

50. Despite recognizing its duty to do so, on information and belief, Defendants have not implemented reasonable cybersecurity safeguards or policies to protect its consumers' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendants left significant vulnerabilities in their systems for cybercriminals to exploit and gain access to consumers' PII.

51. For example, as evidenced by the Data Breach's occurrence, the infiltrated network was not protected by sufficient multi-layer data security technologies or effective firewalls.

52. Similarly, based on the delayed discovery of the Data Breach, it is evident that the infiltrated network, that Defendant allowed to store Plaintiffs' PII, did not have sufficiently effective endpoint detection.

53. Further, the fact that PII was acquired in the Data Breach demonstrates that the PII contained in the Defendants' network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

54. Plaintiffs and Class Members entrusted Defendants with sensitive and confidential information, including their PII which includes information that is static, does not change, and can be used to commit a myriad of financial crimes.

55. Plaintiffs and Class Members relied on Defendants to keep their PII confidential and securely maintained, to use their PII for authorized purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand Defendants safeguard their PII.

56. The unencrypted PII of Plaintiffs and Class Members that was exfiltrated in this Breach will likely end up for sale on the dark web as that is the *modus operandi* of hackers (including the threat actor Alphv/BlackCat here). 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. In turn, unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

57. Defendants 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.

The Data Breach Was Foreseeable

58. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in industries that collect and maintain large amounts of PII preceding the date of the breach.

59. Considering recent high profile data breaches at other related companies, Defendants knew or should have known that their electronic records and the PII that it stored and maintained would be targeted by cybercriminals and ransomware attack groups.

60. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[16]

[16] *See* 2021 Data Breach Annual Report, ITRC 6 (Jan. 2022), available at https://www.idtheftcenter.org/notified.

Defendants Had an Obligation to Protect the PII

61. Defendants' failure to adequately secure Plaintiffs' and Class Members' PII breaches duties they owe Plaintiffs and Class Members under statutory and common law. Moreover, Plaintiffs and Class Members surrendered their highly sensitive personal data to Defendants under the implied condition that Defendants would keep it private and secure. Accordingly, Defendants also have an implied duty to safeguard their data, independent of any statute.

62. Defendants were prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (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 the FTC Act. S*ee, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

63. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Defendants.

64. In addition to its obligations under federal and state laws, Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class Members to provide reasonable security,

including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Plaintiffs and Class Members.

65. Defendants owed a duty to Plaintiffs and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the PII in its possession was adequately secured and protected.

66. Defendants owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII in their possession, including not sharing information with other entities who maintained substandard data security systems.

67. Defendants owed a duty to Plaintiffs and Class Members to implement processes that would immediately detect a breach on their data security systems in a timely manner.

68. Defendants owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

69. Defendants owed a duty to Plaintiffs and Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendants.

70. Defendants owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

71. Defendants owed a duty to Plaintiffs and Class Members to encrypt and/or more reliably encrypt Plaintiffs' and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

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

73. Defendants were, or should have been, fully aware of the unique types and the significant volume of data on their network, amounting to, at least, tens of thousands of individuals' PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

Value of PII

74. The PII of individuals remains of high value to criminals, as evidenced by the prices criminals will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[17] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[18]

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

[18] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the dark*

Criminals can also purchase access to entire company data breaches from $900 to $4,500.[19]

75. Based on the foregoing, the information compromised in the Data Breach, including full names matched with Social Security numbers, 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.

76. 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."[20]

77. 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.

78. The fraudulent activity resulting from the Data Breach may not come to light for years as there may be a time lag between when harm occurs versus when it is

---

web, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[19] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

[20] Time 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.

discovered, and also between when the 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 has 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.[21]

79. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendants' 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.

80. Plaintiffs' and Class Members' PII has already been posted on the dark web by the Alphv/BlackCat group. Thus, Plaintiffs' and Class Members' have all had their data misused and exposed to numerous unauthorized criminals who can commit identity theft and monetize the information in countless nefarious ways.

81. Plaintiffs and Class Members now face a lifetime of constant surveillance of their financial and personal records, credit monitoring, and loss of rights. Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of

[21] *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf.

their PII.

82. Defendants have acknowledged the risk and harm caused to Plaintiffs and Class Members as a result of the Data Breach. Defendants, to date, have offered Plaintiffs and Class Members abbreviated, non-automatic credit monitoring services. The limited credit monitoring is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly considering the PII at issue here. Moreover, Defendants put the burden squarely on Plaintiffs and Class Members to enroll in the inadequate monitoring services.

Defendants Failed to Properly Protect Plaintiffs' and Class Members' PII

83. Defendants could have prevented this Data Breach by properly securing and encrypting the systems containing the PII of Plaintiffs and Class Members. Alternatively, Defendants could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

84. Defendants' negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendants to protect and secure sensitive data they possess.

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

86. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without

authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[22]

87. The ramifications of Defendants' failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for their respective lifetimes.

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

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

[22] *See generally Fighting Identity Theft With the Red Flags Rule: A How-To Guide for Business*, FED. TRADE COMM., https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different

organizational units.[23]

89. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) ….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques.

[23] *Id.* at 3-4.

> You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
>
> - **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[24]

90. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> **Secure internet-facing assets**
>
> - Apply latest security updates;
> - Use threat and vulnerability management;
> - Perform regular audit; remove privileged credentials;
>
> **Thoroughly investigate and remediate alerts**
>
> - Prioritize and treat commodity malware infections as potential full compromise;
>
> **Include IT Pros in security discussions**
>
> - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
>
> **Build credential hygiene**
>
> - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

[24] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware.

Apply principle of least-privilege

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

Harden infrastructure

- Use Windows Defender Firewall;
- Enable tamper protection;
- Enable cloud-delivered protection;
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[25]

91. Moreover, given that Defendants were storing the PII of Plaintiffs and Class Members, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

92. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of Plaintiffs and Class Members.

93. As a result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII.

[25] *See Human-operated ransomware attacks: A preventable disaster*, Microsoft (Mar. 5, 2020). https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

94. Because Defendants failed to properly protect and safeguard Plaintiffs' and Class Members' PII, an unauthorized third party was able to access Defendants' network, and access Defendants' database and system configuration files and exfiltrate that data.

Defendants Failed to Comply with Industry Standards

95. As shown above, experts studying cyber security routinely identify companies in the energy industry as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

96. Several best practices have been identified that at a minimum should be implemented by energy service providers like Defendants, including, but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

97. Other best cybersecurity practices that are standard in the energy 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; and training staff regarding critical points.

98. Defendants 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.

99. The foregoing frameworks are existing and applicable industry standards in the energy services industry, and Defendants failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

100. Upon information and belief, Defendants failed to comply with one or more of the foregoing industry standards.

Defendants' Negligent Acts and Breaches

101. Defendants participated in and controlled the process of gathering the PII from Plaintiffs and Class Members.

102. Defendants therefore assumed and otherwise owed duties and obligations to Plaintiffs and Class Members to take reasonable measures to protect the information, including the duty of oversight, training, instruction, testing of the data security policies and network systems. Defendants breached these obligations to Plaintiffs and Class Members and/or was otherwise negligent because it failed to properly implement data security systems and policies for its energy services network that would adequately safeguard Plaintiffs' and Class Members' PII. Upon information and belief, Defendants' unlawful conduct included, but is not limited to, one or more of the following acts and/or omissions:

a. Failing to design and maintain an adequate data security system to reduce the risk of data breaches and protect Plaintiffs' and Class Members' PII;

b. Failing to properly monitor its data security systems for data security vulnerabilities and risk;

c. Failing to test and assess the adequacy of its data security system;

d. Failing to develop adequate training programs related to the proper handling of emails and email security practices;

e. Failing to develop and put into place uniform procedures and data security protections for its network;

f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

g. Failing to ensure or otherwise require that it be compliant with FTC guidelines for cybersecurity;

h. Failing to ensure or otherwise require that it was adhering to one or more of industry standards for cybersecurity discussed above;

i. Failing to implement or update antivirus and malware protection software in need of security updating;

j. Failing to require encryption or adequate encryption on its data systems;

k. Otherwise negligently and unlawfully failing to safeguard Plaintiffs' and Class Members' PII provided to Defendants, which in turn allowed cyberthieves to access its IT systems.

COMMON INJURIES & DAMAGES

103. As result of Defendants' ineffective and inadequate data security practices, Plaintiffs and Class Members now face a present and ongoing risk of fraud and identity theft.

104. Due to the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to 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) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution or loss of value of their PII; and (i) the continued risk to their PII, which remains in Defendants' possession, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

The Risk of Identity Theft to Plaintiffs and Class Members Is Present and Ongoing

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 are often the starting point for these additional targeted attacks on the victims.

108. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[26] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is entirely different: ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[27] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

109. A sophisticated black market exists on the dark web where criminals can buy

[26]Louis DeNicola, *What Is the dark web?*, Experian (May 12, 2021), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

[27] *Id.*

or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at issue here.[28] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, Social Security numbers, dates of birth, and medical information.[29] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[30]

110. Social Security numbers, for example, are among the worst kinds of personal information to have stolen because they may be put to numerous serious 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 is the case here, 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

[28] *What is the dark web?* – Microsoft 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

[29] *Id.*

[30] *Id.*

> assuming your identity can cause a lot of problems.[31]
>
> 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.

111. Even then, new a Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link 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."[32]

112. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's

---

[31] Social Security Administration, *Identity Theft and Your Social Security Number* (2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[32] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

Social Security number to apply for additional credit lines.[33]

113. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[34]

114. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[35] Defendants did not rapidly report to Plaintiffs and Class Members that their PII had been stolen.

115. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

116. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit

---

[33] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[34] *See 2019 Internet Crime Report*, FBI (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

[35] *Id.*

accounts, open new ones, and dispute charges with creditors.

117. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiffs and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

118. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[36]

119. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on

[36] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), FTC (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[37]

120. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout. The FTC treats 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(a) of the FTC Act.[38]

121. Defendants' failure to properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

122. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming

[37] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

[38] *See, e.g.*, *Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices.

a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

123. Thus, due to Defendants' admitted recognition of the actual and imminent risk of identity theft, Defendants offered Plaintiffs and Class Members abbreviated, non-automatic credit monitoring services.

124. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

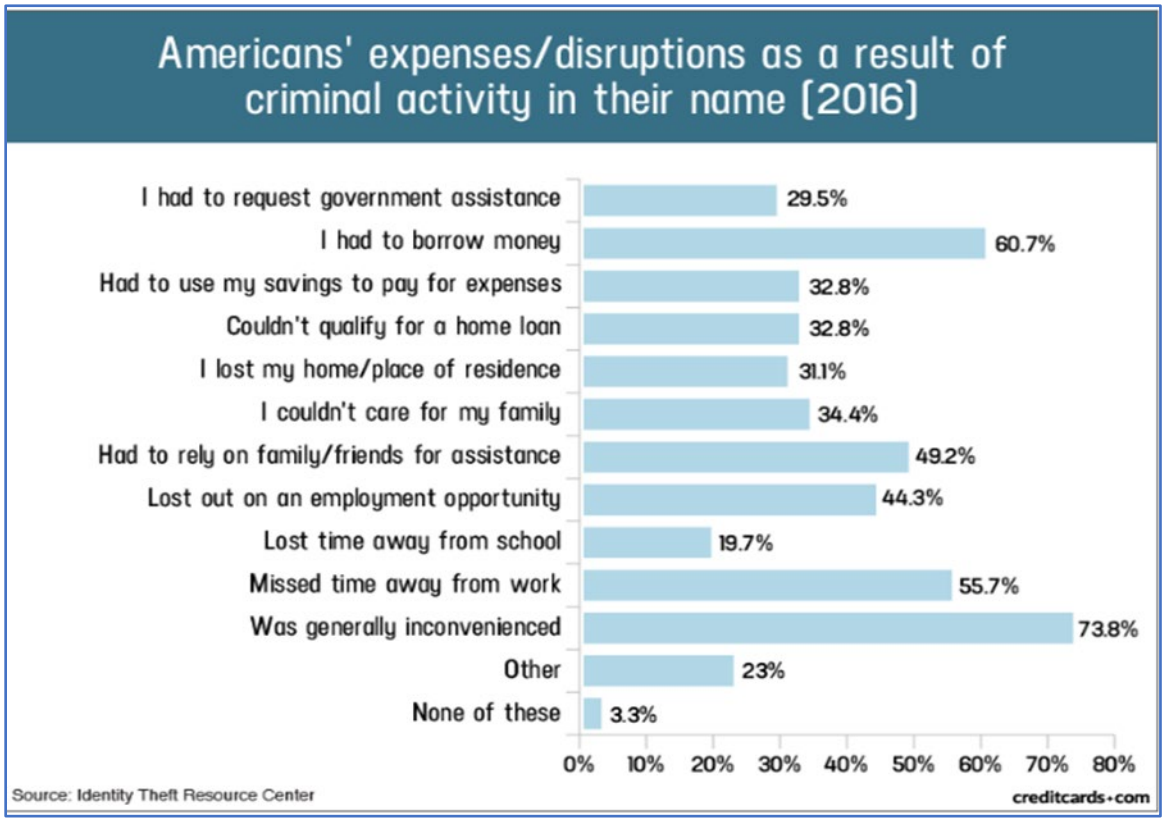
125. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[39]

126. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial

[39] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOBAT, THE FULL EXTENT IS UNKNOWN (2007) ("GAO Report"), available at https://www.gao.gov/new.items/d07737.pdf.

information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[40]

127. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[41]



[40] *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps.

[41] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://web.archive.org/web/20190304002224/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

128. Indeed, the FTC recommends that identity theft victims take several steps and spend time 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 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[42]

Diminution of Value of the PII

129. PII is a valuable property right.[43] Its value is axiomatic, considering the value of data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond a doubt that PII has considerable market value.

130. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves.

131. PII can sell for as much as $363 per record according to the Infosec

[42] *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps.

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

Institute.[44]

132. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data, such as PHI, sells for $50 and up on the dark web.[45]

133. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[46] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[47, 48] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[49]

134. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and

---

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

[45] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

[46] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LA Times (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[47] https://datacoup.com (last visited Dec. 12, 2023).

[48] https://digi.me/how (last visited Dec. 12, 2023).

[49] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

diminished in its value by its unauthorized and potential release onto the dark web, where it may soon be available and holds significant value for the threat actors.

Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

135. To date, Defendants have done little to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach.

136. The abbreviated, non-automatic credit monitoring offered to persons whose PII was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face ongoing identity theft and financial fraud for the remainder of their lives. Defendants also places the burden squarely on Plaintiffs and Class Members by requiring them to independently sign up for that service, as opposed to automatically enrolling all victims of this Data Breach.

137. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, and the *modus operandi* of cybercriminals, 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.

138. It must be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

139. 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.

140. 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.[50] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

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

142. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year, or more, per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendants' failure to safeguard their PII.

Injunctive Relief Is Necessary to Protect against Future Data Breaches

[50] *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.

143. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

PLAINTIFFS' INDIVIDUAL EXPERIENCES

Plaintiff Hernandez's Experience

144. Plaintiff Hernandez received a breach notice letter from Defendants dated December 22, 2023, informing him that his PII, including his name, Social Security number, address, and loan number was identified as having been compromised in the Data Breach.

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

146. Because of the Data Breach, Plaintiff Hernandez Private Information is now in the hands of cybercriminals.

147. Plaintiff suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

148. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Hernandez is now imminently at risk of

crippling future identity theft and fraud.

149. As a result of the Data Breach, Plaintiff has had no choice but to spend numerous hours attempting to mitigate the harm caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff has devoted time to investigating the Data Breach, reviewing account statements and other personal information, and taking other protective and ameliorative steps in response to the Data Breach. All of these actions have taken several hours away from Plaintiff Hernandez's valuable time that he otherwise would have spent on other activities.

150. The letter Plaintiff received from Defendants specifically directed him to take the actions described above.

151. As a result of the Data Breach, Plaintiff Hernandez has experienced stress and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information.

152. Plaintiff Hernandez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

153. Given the time Plaintiff Hernandez has lost investigating this Data Breach, taking steps to understand its full scope, determining the appropriate remedial steps, contacting counsel, etc., coupled with Plaintiff Hernandez's resultant and naturally foreseeable fears/concerns for the use of Plaintiff Hernandez's valuable PII, the damages articulated more specifically above are far from the full extent of the harm thereto.

Plaintiff Bat's Experience

154. Plaintiff Bat received a breach notice letter from Defendants dated December 22, 2023, informing her that her PII, including her name, Social Security number, address, and loan number was identified as having been compromised in the Data Breach.

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

156. Because of the Data Breach, Plaintiff Bat's Private Information is now in the hands of cybercriminals.

157. Plaintiff Bat suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

158. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff Bat is now imminently at risk of crippling future identity theft and fraud.

159. As a result of the Data Breach, Plaintiff Bat has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Bat has devoted time to investigating the Data Breach, reviewing account statements, and taking other protective and ameliorative steps in response to the Data Breach. All of these actions have taken several hours away from Plaintiff Bat's valuable time that she otherwise would have spent

on other activities.

160. The letter Plaintiff Bat received from Defendants specifically directed her to take the actions described above.

161. As a result of the Data Breach, Plaintiff Bat has experienced stress and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information.

162. Plaintiff Bat anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

163. Given the time Plaintiff Bat has lost investigating this Data Breach, taking steps to understand its full scope, determining the appropriate remedial steps, contacting counsel, etc., coupled with Plaintiff Bat's resultant and naturally foreseeable fears/concerns for the use of Plaintiff Bat's valuable PII, the damages articulated more specifically above are far from the full extent of the harm thereto.

CLASS ALLEGATIONS

164. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

165. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All United States residents who were sent a Notice Letter by Defendants notifying them that their PII was actually or potentially accessed or acquired during the Data Breach.

166. Plaintiff Bat also seeks to represent a California Subclass defined as follows:

> All California residents who were sent a Notice Letter by Defendants notifying them that their PII was actually or potentially accessed or acquired during the Data Breach.

167. The Nationwide Class and the California Subclass are collectively referred to herein as the "Class."

168. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

169. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

170. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are at least multiple thousands of individuals who were notified by Defendants of the Data Breach. According to the report submitted to the Maine Attorney General's office, 1,316,938

individuals had their PII compromised in this Data Breach.[51] The identities of Class Members are ascertainable through Defendants' records, Class Members' records, publication notice, self-identification, and other means.

171. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendants had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendants had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;

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

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs

[51] See Data Breach Notifications, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/0c96d450-be94-40b9-92ad-6c8e1cf64ef8.shtml.

and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

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

k. Whether Defendants violated the consumer protection statutes invoked herein;

l. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;

m. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

n. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

172. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendants' misfeasance.

173. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds

generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

174. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

175. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): 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 Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

176. 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 Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

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

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

180. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

181. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendants on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendants breached the implied contract;

f. Whether Defendants adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

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

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

CAUSES OF ACTION

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

182. Plaintiffs repeat, reallege, and incorporate paragraphs 1-181 as if fully set forth herein.

183. Defendants were entrusted with Plaintiffs and Class Members' PII as a condition of Plaintiffs' and Class Members' mortgage loans with the understanding that Defendants would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

184. Defendants have 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.

185. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

186. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the PII of Plaintiffs and the Class in Defendants' possession was adequately secured and protected.

187. Defendants also had a duty to exercise appropriate clearinghouse practices to remove PII they were no longer required to retain.

188. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Class.

189. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential PII, a necessary part of obtaining services and/or employment from Defendants.

190. Defendants were subject to an "independent duty," untethered to any contract

between Defendants and Plaintiffs or the Class.

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

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

193. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and the Class. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and the Class, including basic encryption techniques freely available to Defendants.

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

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

196. Defendants had and continue to have a duty to adequately disclose that the PII of Plaintiffs and the Class within Defendants' possession might have been

compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow 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.

197. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Class.

198. Defendants have 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.

199. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Class during the time the PII was within Defendants' possession or control.

200. Defendants improperly and inadequately safeguarded the PII of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

201. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Class in the face of increased risk of theft.

202. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of PII.

203. Defendants breached their duty to exercise appropriate clearinghouse

practices by failing to remove PII they were no longer required to retain pursuant to regulations.

204. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and the Class the existence and scope of the Data Breach.

205. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the PII of Plaintiffs and the Class would not have been compromised.

206. There is a close causal connection between Defendants' 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 Nationwide Class. The PII of Plaintiffs and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

207. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

208. Defendants 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. Defendants' 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.

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

210. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

211. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its 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.

212. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which

remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

213. As a direct and proximate result of Defendants' 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.

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

215. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class)

216. Plaintiffs repeat, reallege, and incorporate paragraphs 1-215 as if fully set forth herein.

217. Plaintiffs and Class Members provided their PII to Defendants as part of its regular business practices.

218. Plaintiffs and Class Members entrusted their PII to Defendants. In doing so, Plaintiffs and the Class entered into implied contracts with Defendants by which it 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.

219. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their PII to Defendants with the reasonable understanding that their PII would be adequately protected from foreseeable threats. This inherent understanding exists independent of any other law or contractual obligation any time that highly sensitive PII is exchanged as a condition of receiving services. It is common sense that but for this implicit and/or explicit agreement, Plaintiffs and Class Members would not have provided their PII to Defendants.

220. Based on Defendants' conduct, representations (including those in FNF's Privacy Policy), legal obligations, and acceptance of Plaintiffs' and the Class Members' Private Information, Defendants had an implied duty to safeguard their Private Information through the use of reasonable industry standards.

221. Indeed, the Privacy Policy posted on Defendants' website reassures: "Defendants recognizes that privacy is important to you…. We will not sell, trade,

exchange or otherwise make available any personally identifiable information to any other company or organization not directly affiliated with Defendants."[52]

222. Defendants' conduct and statements confirm that Defendants intended to bind themselves to protect the PII that Plaintiffs and the Class entrusted to Defendants.

223. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants.

224. Defendants breached the implied contracts they made with Plaintiffs and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that PII was compromised as a result of the Data Breach.

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

[52] https://www.Defendantsenergy.com/privacy-policy/ (last visited Dec. 8, 2023).

226. As a result of Defendants' breach of implied contract, Plaintiffs and Class Members are entitled to and demand actual, consequential, and nominal damages.

COUNT III
Unjust Enrichment
(On behalf of Plaintiffs and the Class)

227. Plaintiffs repeat, reallege and incorporate paragraphs 1-226 as if fully set forth herein.

228. Plaintiffs bring this claim in the alternative to their breach of implied contract claim.

229. Plaintiffs and Class Members conferred a monetary benefit upon Defendants in the form of direct or indirect payment for services. The money received by Defendants was supposed to be used by Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

230. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII.

231. Defendants were also enriched from the value of Plaintiffs' and Class Members' PII. PII has independent value as a form of intangible property. Defendants also derive value from this information because it allows Defendants to operate their business and generate revenue.

232. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security

measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

233. Under the principles of equity and good conscience, Defendants should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

234. Defendants acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

235. If Plaintiffs and Class Members knew that Defendants had not secured their PII, they would not have agreed to provide their PII to Defendants.

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

237. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) 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; (vi) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as

Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

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

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

240. Plaintiff Bat ("Plaintiff" for purposes of this count) and the California Subclass repeats, realleges, and incorporates paragraphs 1-239 as if fully set forth herein.

241. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA.

242. Defendants are "business[es]" under § 1798.140(d) in that they are organized for profit or financial benefit of their shareholders or other owners, with gross revenues in excess of $25 million.

243. Plaintiff and California Subclass Members are covered "consumers" under § 1798.140(i) in that they are natural persons who are California residents.

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

245. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the California Subclass Members' personal information and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass Members. Specifically, Defendants subjected Plaintiff's and the California

Subclass Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendants' violations of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

246. As a direct and proximate result of Defendants' violation of their duties, the unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and California Subclass Members' personal information included exfiltration, theft, or disclosure through Defendant's servers, systems, and website, and/or the dark web, where hackers further disclosed the personal identifying information alleged herein.

247. As a direct and proximate result of Defendants' acts, Plaintiff and the California Subclass Members were injured and lost money or property, including but not limited to the loss of Plaintiff and California Subclass Members' legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

248. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages."

249. At this time, Plaintiff and California Class Members seek only actual pecuniary damages suffered as a result of Defendant's violations of the CCPA, injunctive and declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and any other relief the court deems proper.

250. Concurrently with the filing of this Complaint, Plaintiff is providing written notice to Defendant identifying the specific provisions of this title he alleges it has violated. If within 30 days of Plaintiff's written notice to Defendant it fails to "actually cure" its violations of Cal. Civ. Code § 1798.150(a) and provide "an express written statement that the violations have been cured and that no further violations shall occur," Plaintiff will amend this complaint to also seek the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(b).

COUNT V
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW,
Cal. Bus. & Prof. Code §17200 *et seq.*
(On Behalf of Plaintiff Bat and the California Subclass)

251. Plaintiff Bat ("Plaintiff" for purposes of this count) repeats, realleges, and incorporates paragraphs 1-250 as if fully set forth herein.

252. Defendants are "person[s]" as defined by Cal. Bus. & Prof. Code § 17201.

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

254. Defendants' "unfair" acts and practices include:

a. failing to implement and maintain reasonable security measures to protect Plaintiff and California Subclass Members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Defendants Data Breach. Defendants failed to

identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. Defendants' failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. Defendants' failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendants' inadequate security, consumers could not have reasonably avoided the harms that Defendants caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

255. Defendants has engaged in "unlawful" business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45, and California common law.

256. Defendants' unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass Members' personal information, which was a direct and proximate cause of the Defendants Data Breach;

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

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

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and California Subclass Members' personal information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and California Subclass Members' personal information; and

g. Omitting, suppressing, and concealing the material fact that they did not

comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

257. Defendants' representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Defendants' data security and ability to protect the confidentiality of their personal information.

258. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass Members were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

259. Defendants' violations were, and are, willful, deceptive, unfair, and unconscionable.

260. Plaintiff and California Subclass Members have lost money and property as a result of Defendants' conduct in violation of the UCL, as stated herein and above. Plaintiff and California Subclass Members paid more than they would have based upon the belief that Defendants would implement reasonable data security practices and suffered from the lost benefit of their bargain with Defendants.

261. By deceptively storing, collecting, and disclosing their personal information, Defendants took money or property from Plaintiff and California Subclass Members.

262. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff and California Subclass Members' rights.

263. Plaintiff and California Subclass Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;

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

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendants to delete, destroy, and purge the PII of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendants from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

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

security auditors;

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

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

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

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

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and Class Members;

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

xiii. requiring Defendants to implement a system of tests to assess its

respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

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

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

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

D. For an award of damages, including, but not limited to, actual, consequential,

and nominal damages, as allowed by law in an amount to be determined;

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

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: January 5, 2024

/s/Jessica Wallace

Jessica Wallace (Bar No. 1008325)
SIRI & GLIMSTAD LLP
20200 West Dixie Highway, Suite 902
Aventura, FL 33180
T: (786) 244-5660
E: jwallace@sirillp.com

A. Brooke Murphy
(application for *pro hac vice* forthcoming)
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
T: (405) 389-4989
E: abm@murphylegalfirm.com

Counsel for Plaintiffs and the Putative Class

ClassAction.org
