IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF FLORIDA
JACKSONVILLE DIVISION

GREGORY ARROWSMITH, on behalf of himself and all others similarly situated, Plaintiff, v. FIDELITY NATIONAL FINANCIAL INC., And LOANCARE, LLC, Defendants.	CASE NO. **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff, Gregory Arrowsmith ("Plaintiff"), on behalf of himself and all others similarly situated, states as follows for his class action complaint against Defendants, Fidelity National Financial Inc. ("FNF") and LoanCare, LLC ("LoanCare") (collectively with FNF, "Defendants"):

INTRODUCTION

1. On November 19, 2023, FNF, a Fortune 500 company that claims to be a leading provider of title insurance and settlement services for the mortgage and real estate industries[1], lost control over its computer network and the highly sensitive personal information stored on the computer network in a data breach by cybercriminals ("Data Breach"). On information and belief, the Data Breach has impacted a staggering 1.3 million thousand consumers.

[1] https://www.investor.fnf.com/

2. LoanCare, a self-touted "national recognized leader in full-service subservicing to the mortgage industry"[2] is a FNF company and direct subsidiary of FNF. LoanCare chose to allow FNF access and control over its consumers' highly sensitive information.

3. Due to Defendants' intentionally obfuscating language, it is unclear when the Data Breach precisely occurred and how long cybercriminals had unfettered access to Plaintiff's and the Class's highly sensitive information. Following an internal investigation, Defendants learned cybercriminals gained unauthorized access to consumers' personally identifiable information ("PII"), including but not limited to their name, address, Social Security Number, and Loan number.

4. On or about December 22, 2023–over a month after the Data Breach was discovered– Defendants finally notified Plaintiff and Class Members about the Data Breach ("Breach Notice"). An example of the Breach Notice is attached as Exhibit A.

5. Upon information and belief, cybercriminals were able to breach Defendants' systems because Defendants failed to adequately train their employees on cybersecurity, failed to adequately monitor their agents, contractors, vendors, and suppliers in handling and securing the PII of Plaintiff, and failed to maintain reasonable security safeguards or protocols to protect the Class's PII—rendering them easy targets for cybercriminals.

6. Defendants' Breach Notice obfuscated the nature of the breach and the threat

[2] https://fnf.com/companies/mortgage-real-estate-services/#LoanCare

it posted—refusing to tell its consumers how many people were impacted, how the breach happened, when the Breach happened, or why it took the Defendants over a month to begin notifying victims that cybercriminal had gained access to their highly private information.

7. Defendants' failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

8. Defendants knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

9. In failing to adequately protect consumers' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendants violated state law and harmed a staggering number of consumers.

10. Plaintiff and the Class are victims of Defendants' negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendants with their PII. But Defendants betrayed that trust. Defendants failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiff is a Data Breach victim.

12. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiff and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

PARTIES

13. Plaintiff, Gregory Arrowsmith, is a natural person and citizen of California, residing in Orange, California, where he intends to remain.

14. Defendant Fidelity National Financial, Inc. is incorporated in Delaware with its principal place of business at 601 Riverside Ave., Building 5, Jacksonville, Florida 32204. Defendant FNF is therefore a Delaware and Florida corporation.

15. Defendant LoanCare, LLC is incorporated in Delaware with its principal place of business at 3673 Sentara Way, Virginia Beach, Virginia 23452. Defendant LoanCare is therefore a Delaware and Virginia corporation.

JURISDICTION & VENUE

16. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are over 100 putative Class Members.

17. This Court has personal jurisdiction over Defendants because at least one Defendant is headquartered in Florida, and both Defendants regularly conducts business in Florida. Plaintiff and Defendants are citizens of different states.

18. Venue is proper in this Court under because at least one Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

FNF and LoanCare

19. FNF, is a Fortune 500 company that claims to be a leading provider of title

insurance and settlement services for the mortgage and real estate industries.[3] It boasts a staggering annual revenue of $10.87 billion.[4]

20. LoanCare is a self-proclaimed "leading national provider of full-service subservicing and interim subservicing to the mortgage industry and has offered its expertise and best practices in providing servicing solutions for others since 1991."[5] At the present time, LoanCare subservices over 1.2 million loans in 50 states, approximating $390 billion in loan balances.[6] LoanCare boasts an annual revenue of $618.7 million.[7]

21. As part of its business, Defendants receives, collects, and maintains the PII of millions of its consumers. In doing so, Defendants implicitly promise to safeguard their PII.

22. After collecting their consumers' PII, Defendants maintain the PII in their computer systems.

23. In collecting and maintaining consumers' highly sensitive data, Defendants agreed they would safeguard the data in accordance with their internal policies as well as state law and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

24. Indeed, Defendants understood the importance of adequate cybersecurity measures, declaring in their Privacy Policy that "[FNF] and its majority-owned subsidiary

[3] https://www.investor.fnf.com/
[4] https://stockanalysis.com/stocks/fnf/revenue/
[5] https://www.linkedin.com/company/loancare/
[6] *Id.*
[7] https://www.zoominfo.com/c/loancare-llc/63505683

companies [including LoanCare] respect and are committed to protecting your privacy."[8]

25. Defendants further assures their consumers that "we maintain physical, electronic, and procedural safeguards to protect your Personal Information."[9]

26. Defendants understood the need to protect their consumers' PII and prioritize their data security.

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

Defendants Fails to Safeguard Consumers' PII

28. Plaintiff is Defendants' consumer and client. As a condition of receiving Defendants' services, Plaintiff provided his name, home address, loan information, and Social Security Number. Defendants used that PII to facilitate their services to Plaintiff and required Plaintiff to provide that PII in order to obtain their services.

29. On information and belief, Defendants collects and maintains consumers' unencrypted PII in their computer systems.

30. According to the Breach Notice, Defendants claim that "on or about November 19, 2023, LoanCare, LLC […] became aware of unauthorized access to certain systems within its parent's Fidelity National Financial, Inc information technology

[8] https://fnf.com/privacy-notice
[9] *Id.*

network." Due to Defendants' obfuscating information, the precise dates in which the Data breach occurred and how long cybercriminals had access to Plaintiff's and the Class's most sensitive information is currently unknown.

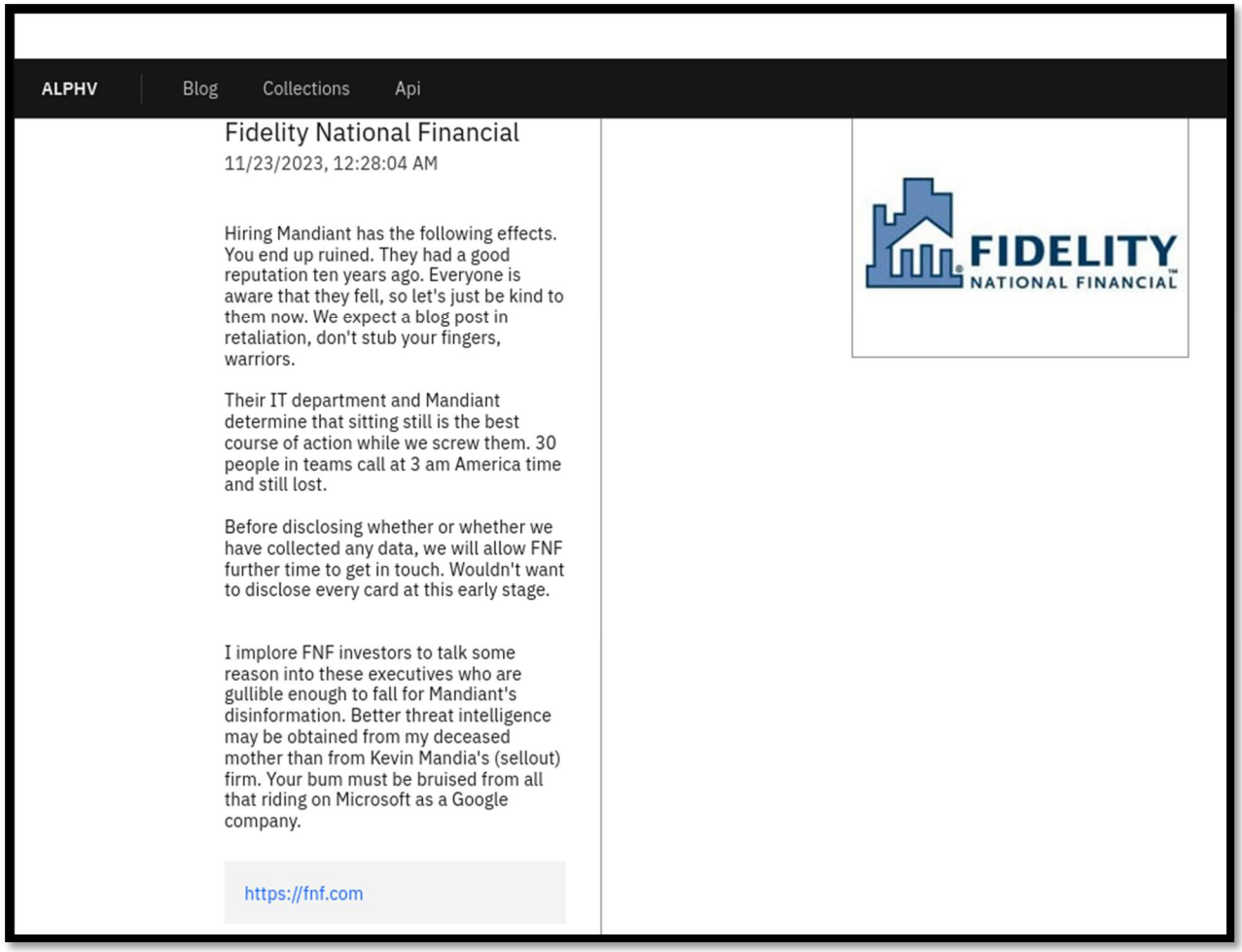
31. Following an internal investigation, Defendants revealed that the cybercriminals "exfiltrated data from certain FNF systems." Ex. A. In other words, the Data Breach investigation revealed FNF's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of millions of its consumers' highly private information. LoanCare knew or should have known that granting FNF access to Plaintiff's PII would result in a Data Breach given FNF's inadequate cybersecurity practices.

32. Additionally, Defendants admitted that PII was actually stolen during the Data Breach confessing that the information was not just accessed, but "exfiltrated" from FNF's system. Ex. A.

33. Through their inadequate security practices, Defendants exposed Plaintiff's and the Class's PII for theft and sale on the dark web.

34. On information and belief, the notorious and aggressive BlackCat, also known as Alphv, ransomware gang took credit for the Data Breach.[10] An incredibly active and successful hacker collective with over 1,000 victims between 2022 and 2023 alone[11], Defendants knew or should have known of the tactics that hackers like BlackCat employ.

[10] https://www.securityweek.com/loancare-notifying-1-3-million-of-data-breach-following-cyberattack-on-parent-company/#:~:text=LoanCare%20told%20the%20Maine%20Attorney,for%20the%20attack%20on%20FNF.
[11] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a



35. With the PII secured and stolen by BlackCat, the hackers then purportedly issued a ransom demand to Defendants. However, Defendants have provided no public information on the ransom demand or payment.

36. On information or belief, 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.[12]

37. On or about December 22, 2023– over a month after the Data Breach was

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

discovered– Defendants finally began notifying Plaintiff and Class Members about the Data Breach.

38. Despite their duties and alleged commitments to safeguard PII, Defendants, self-proclaimed leaders in their industry, did not in fact follow industry standard practices in securing consumers' PII, as evidenced by the Data Breach.

39. Typically, companies who have suffered Data Breaches will, in their Breach Notice, make promises to their consumers regarding implementing additional safeguards and security to prevent such breaches from occurring again. Not Defendants. Instead, Defendants places the onus on Plaintiff, merely instructing Plaintiff to review "further steps you can take" as suggested in the Breach Notice and to call Defendants' listed number for any further questions. Ex. A.

40. On information and belief, Defendants' listed phone number does not work, and consumers have been unable to reach a representative for additional information.

41. Through their Breach Notice, Defendants recognized the actual imminent harm and injury that flowed from the Data Breach, so they encouraged breach victims to "review and monitor your account for suspicious activity" and to be "be especially vigilant for the next 12 to 24 months and that you promptly report incidents of suspected identity theft to your financial institution." Ex. A.

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

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

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

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

The Data Breach was a Foreseeable Risk of Which Defendants were on Notice.

46. It is well known that PII, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

47. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[13]

48. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook

[13] Data breaches break record in 2021, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed May 04, 2023).

(267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Instron knew or should have known that its electronic records would be targeted by cybercriminals.

49. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

50. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendants failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

51. In the years immediately preceding the Data Breach, Defendants knew or should have known that Defendants' computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

52. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the

transportation sector."[14]

53. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[15]

54. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[16]

55. This readily available and accessible information confirms that, prior to the Data Breach, Defendants knew or should have known that (i) ransomware actors were targeting entities such as Defendants, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendants, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

56. In light of the information readily available and accessible on the internet before the Data Breach, Defendants, having elected to store the unencrypted PII of

[14] https://www.ic3.gov/Media/Y2019/PSA191002
[15] https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/
[16] https://www.cisa.gov/stopransomware/ransomware-guide

thousands of their consumers in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendants' type of business had cause to be particularly on guard against such an attack.

57. Before the Data Breach, Defendants knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendants.

58. Prior to the Data Breach, Defendants knew or should have known that they should have encrypted their consumers' Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Plaintiff's Experience and Injuries

59. Plaintiff is a consumer using Defendants' services and received Defendants' breach notice on or about December 22, 2023.

60. As a condition of receiving Defendants' services, Plaintiff provided his name, home address, loan information, and Social Security Number. Defendants used that PII to facilitate their services to Plaintiff and required Plaintiff to provide that PII in order to obtain their services.

61. Plaintiff provided his PII to Defendants and trusted that they would use reasonable measures to protect it according to its internal policies and state and federal law.

62. Defendants deprived Plaintiff of the earliest opportunity to guard himself

against the Data Breach's effects by failing to notify him about it for over a month.

63. Plaintiff does not recall ever learning that his PII was compromised in a data breach incident, other than the breach at issue in this case.

64. As a result of its inadequate cybersecurity, Defendants exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

65. Plaintiff suffered actual injury from the exposure of his PII —which violates his rights to privacy.

66. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendants was required to adequately protect.

67. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, placing a credit freeze through the three main credit bureaus, and monitoring his credit information.

68. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

69. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendants delay in informing Plaintiff and Class Members about the Data Breach.

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

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

71. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendants.

72. As a result of Defendants' failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the class have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended 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 and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the PII in their possession.

73. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

74. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

75. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

76. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

77. One such example of criminals using PII for profit is the development of

"Fullz" packages.

78. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

79. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and members of the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

80. Defendants disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

81. Defendants' failure to properly notify Plaintiff and the Class of the Data

Breach exacerbated Plaintiff's and the Class's injuries 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.

Defendants failed to adhere to FTC guidelines.

82. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendants, should employ to protect against the unlawful exposure of PII.

83. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

84. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

85. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

87. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Failed to Follow Industry Standards

88. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendants. These industry standards include: 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.

89. Other industry standard best practices 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.

90. 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.

91. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendants opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

92. Plaintiff sues on behalf of himself and the proposed nationwide class ("Class") and state subclass ("Subclass"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> **Nationwide Class: All individuals residing in the United States whose PII was compromised in the Data Breach, including all those who received notice of the breach.**
>
> **California Subclass: All individuals residing in California whose PII was compromised in the Data Breach, including all those who received notice of the breach.**

93. Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any of Defendants' officer's or directors, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

94. Plaintiff reserves the right to amend the class definition.

95. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believes that the proposed Class includes a staggering 1.3 million individuals who have been damaged by Defendants' conduct as alleged herein.

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendants' possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. His interests do not conflict with the Class's interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

ii. 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;

iii. Whether Defendants were negligent in maintaining, protecting, and securing PII;

iv. Whether Defendants breached contract promises to safeguard Plaintiff's and the Class's PII;

v. Whether Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendants' Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

96. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(Against Defendants On Behalf of Plaintiff and the Class)

97. Plaintiff and members of the Class incorporate the allegations in paragraphs 1-96 as if fully set forth herein.

98. Defendants owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the PII in their care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

99. Defendants owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendants' failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

100. Defendants owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendants also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

101. Defendants owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom

Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Defendants actively sought and obtained Plaintiff's and the Class's personal information and PII.

102. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendants hold vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the PII—whether by malware or otherwise.

103. PII is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

104. Defendants breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

105. Defendants' breach of their common-law duties to exercise reasonable care

and their failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

Count II
Negligence *Per Se*
(Against Defendants On Behalf of Plaintiff and the Class)

106. Plaintiff and members of the Class incorporate the allegations in paragraphs 1-96 as if fully set forth herein.

107. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants have a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

108. 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 consumers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff's and the Class's sensitive PII.

109. Defendants violated their duty under 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 Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

110. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

111. Defendants have a duty to Plaintiff and the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class's PII.

112. Defendants breached their duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

113. Defendants' violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se.*

114. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and the Class would not have been injured.

115. The injury and harm suffered by Plaintiff and the Class were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties and that their breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

116. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

Count III
Breach of Fiduciary Duty
(Against Defendants On Behalf of Plaintiff and the Class)

117. Plaintiff and members of the Class incorporate the allegations in paragraphs 1-96 as if fully set forth herein.

118. Given the relationship between Defendants and Plaintiff and Class Members, where Defendants became guardian of Plaintiff's and Class Members' PII, Defendants became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants did and does store.

119. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendants' relationship with them—especially to secure their PII.

120. Because of the highly sensitive nature of the PII, Plaintiff and Class Members would not have entrusted Defendants, or anyone in Defendants' position, to retain their PII

had they known the reality of Defendants' inadequate data security practices.

121. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class Members' PII.

122. Defendants also breached their fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

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

Count IV
Breach of Implied Contract
(Against Defendants On Behalf of Plaintiff and the Class)

124. Plaintiff and members of the Class incorporate the allegations in paragraphs 1-96 as if fully set forth herein.

125. Plaintiff and the Class delivered their PII to Defendants as part of the process of obtaining services provided by Defendants.

126. Plaintiff and Class Members entered into implied contracts with Defendants under which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendants an implied covenant of good faith and fair dealing by which Defendants was required to perform its obligations and manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data

to Defendants.

127. In providing their PII, Plaintiff and Class Members entered into an implied contract with Defendants whereby Defendants, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' PII.

128. In delivering their PII to Defendants, Plaintiff and Class Members intended and understood that Defendants would adequately safeguard that data.

129. Plaintiff and the Class Members would not have entrusted their PII to Defendants in the absence of such an implied contract.

130. Defendants accepted possession of Plaintiff's and Class Members' PII.

131. Had Defendants disclosed to Plaintiff and Class Members that Defendants did not have adequate computer systems and security practices to secure consumers' PII, Plaintiff and members of the Class would not have provided their PII to Defendants.

132. Defendants recognized that consumers' PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

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

134. Defendants breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard their data.

135. Defendants breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their PII.

136. As a direct and proximate result of the breach of the contractual duties,

Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendants promised when Plaintiff and the proposed class entrusted Defendants with their PII; and (h) the continued and substantial risk to Plaintiff's and Class Members' PII, which remains in the Defendants' possession with inadequate measures to protect Plaintiff's and Class Members' PII.

Count V
Unjust Enrichment
(Against Defendants On Behalf of Plaintiff and the Class)

137. Plaintiff and members of the Class incorporate the allegations in paragraphs 1-96 as if fully set forth herein.

138. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

139. Plaintiff and Class Members conferred a monetary benefit on Defendants, by providing Defendants with their valuable PII.

140. Defendants enriched themselves by saving the costs they reasonably should

have expended on data security measures to secure Plaintiff's and Class Members' PII.

141. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and the Class, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

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

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

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

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

146. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their PII is used; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited

to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) 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 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 Plaintiff and the Class.

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

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

Count VI
Violation of California's Unfair Competition Law ("UCL")
Unlawful Business Practice
(Cal Bus. & Prof. Code § 17200, et seq.)
(Against Defendants On Behalf of Plaintiff and the California Subclass)

149. Plaintiff and members of the Class incorporate the allegations in paragraphs 1-96 as if fully set forth herein.

150. Plaintiff brings this Count on his own behalf and on behalf of the California Class (the "Class" for the purposes of this Count).

151. Defendants engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

152. Defendants' conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, et seq. (the "CCPA"), and other state data security laws.

153. Defendants stored the PII of Plaintiff and the Class in their computer systems and knew or should have known they did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiff's and the Class's PII secure so as to prevent the loss or misuse of that PII.

154. Defendants failed to disclose to Plaintiff and the Class that their PII was not secure. However, Plaintiff and the Class were entitled to assume, and did assume, that Defendants had secured their PII. At no time were Plaintiff and the Class on notice that their PII was not secure, which Defendants had a duty to disclose.

155. Defendants also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and the Class's nonencrypted and nonredacted PII.

156. Had Defendants complied with these requirements, Plaintiff and the Class would not have suffered the damages related to the data breach.

157. Defendants' conduct was unlawful, in that it violated the CCPA.

158. Defendants' acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the Federal Trade Commission Act.

159. Defendants' conduct was also unfair, in that it violated a clear legislative

policy in favor of protecting consumers from data breaches.

160. Defendants' conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting PII.

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

162. Instead, Defendants made the PII of Plaintiff and the Class accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiff and the Class to an impending risk of identity theft. Additionally, Defendants' conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

163. As a result of those unlawful and unfair business practices, Plaintiff and the Class suffered an injury-in-fact and have lost money or property.

164. The injuries to Plaintiff and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

165. There were reasonably available alternatives to further Defendants' legitimate business interests, other than the misconduct alleged in this complaint.

166. Therefore, Plaintiff and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendants; disgorgement of all profits accruing to Defendants because of their unfair and improper business practices; a permanent injunction enjoining Defendants' unlawful and unfair business activities; and any other equitable relief the Court deems proper.

Count VII
Violation of the California Consumer Records Act
Cal. Civ. Code § 1798.80, et seq.
(Against Defendants On Behalf of Plaintiff and the California Subclass)

167. Plaintiff and members of the Class incorporate the allegations in paragraphs 1-96 as if fully set forth herein.

168. Plaintiff brings this Count on his own behalf and on behalf of the California Class (the "Class" for the purposes of this Count).

169. Under California law, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82.) The disclosure must "be made in the most expedient

time possible and without unreasonable delay" (Id.), but "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82, subdiv. b.)

170. The Data Breach constitutes a "breach of the security system" of Defendants.

171. An unauthorized person acquired the personal, unencrypted information of Plaintiff and the Class.

172. Defendants knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiff and the Class, but waited approximately over a month to notify them. A month was an unreasonable delay under the circumstances.

173. Defendants' unreasonable delay prevented Plaintiff and the Class from taking appropriate measures from protecting themselves against harm.

174. Because Plaintiff and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

175. Plaintiff and the Class are entitled to equitable relief and damages in an amount to be determined at trial.

Count VIII
Violation of the California Consumer Privacy Act
Cal. Civ. Code § 1798.150
(Against Defendants On Behalf of Plaintiff and the California Subclass)

176. Plaintiff and members of the Class incorporate the allegations in paragraphs 1-96 as if fully set forth herein.

177. Plaintiff brings this Count on his own behalf and on behalf of the California

Class (the "Class" for the purposes of this Count).

178. Defendants violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiff and the Class. As a direct and proximate result, Plaintiff's, and the Class's nonencrypted and nonredacted PII was subject to unauthorized access and exfiltration, theft, or disclosure.

179. Defendants are businesses organized for the profit and financial benefit of their owners according to California Civil Code § 1798.140, that collects the personal information of its customers, and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

180. Plaintiff and Class Members seek injunctive or other equitable relief to ensure Defendants hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continues to hold PII, including Plaintiff's and Class members' PII. Plaintiff and Class members have an interest in ensuring that their PII is reasonably protected, and Defendants have demonstrated a pattern of failing to adequately safeguard this information.

181. Pursuant to California Civil Code § 1798.150(b), Plaintiff mailed a CCPA notice letter to Defendants' registered service agents, detailing the specific provisions of the CCPA that Defendants have violated and continues to violate. If Defendants cannot cure within 30 days—and Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

182. As described herein, an actual controversy has arisen and now exists as to whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

183. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendants.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to

be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff hereby demands that this matter be tried before a jury.

Dated: January 4, 2023,

Respectfully Submitted,

/s/*Jonathan B. Cohen*

Jonathan B. Cohen (FL Bar No. 27620)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
3833 Central Ave.
St. Petersburg, FL 33713
Phone: 813-699-4056
Email: jcohen@milberg.com

Samuel J. Strauss*
sam@turkestrauss.com
Raina Borrelli*
raina@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
T: (608) 237-1775
F: (608) 509-4423

* *Pro hac vice forthcoming*

Attorneys for Plaintiff and Proposed Class

EXHIBIT A

LOANCARE®

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: NOTICE OF DATA BREACH

Dear <<First_Name>> <<Last_Name>>:

We are writing to notify you of a recent event that may have impacted your personal information. At this time, we have no indication of fraudulent use of your personal information as a result of this incident. Nevertheless, we are notifying you out of an abundance of caution to explain the circumstances as we understand them and the resources we are making available to you.

What Happened?

On or about November 19, 2023, LoanCare, LLC ("LoanCare"), which performs or has performed loan subservicing functions for your mortgage loan servicer, became aware of unauthorized access to certain systems within its parent's, Fidelity National Financial, Inc. ("FNF"), information technology network. Upon becoming aware of the incident, FNF commenced an investigation with the assistance of third-party experts, notified certain law enforcement and governmental authorities, and began taking measures to assess and contain the incident. The incident has been contained.

The investigation has determined that an unauthorized third party exfiltrated data from certain FNF systems. As part of the review of the potentially impacted data, LoanCare identified that some of your personal information may have been among that data. It is important to note that we have not identified any fraudulent use of your personal information as a result of this incident.

What Information Was Involved?

Based on our investigation, we understand that your Name, Address, Social Security Number, and Loan Number may have been obtained by the unauthorized third party.

What We Are Doing

Upon learning of the incident, we promptly launched an investigation into the nature and scope of the incident and notified law enforcement. We also took measures to further secure our systems. The incident has been contained

To help address concerns you may have about this incident, we have secured the services of Kroll to provide identity monitoring services at no cost to you for twenty-four (24) months. Your identity monitoring services include Credit Monitoring, Web Watcher, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. Additional information describing these services is included on page three of this letter. To activate these services, please take the following steps:

Visit https://enroll.krollmonitoring.com to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (ActivationDeadline)>> to activate your identity monitoring services.

Please reference Membership Number: <<Membership Number (S_N)>>

What You Can Do

Though at this time we have no indication of fraudulent use of your personal information as a result of this incident, it is always advisable to review and monitor your account(s) for suspicious activity. Further steps you can take can be found on the "Additional Ways to Protect Your Identity" document we have included on the following pages.

For More Information

We understand the concern and inconvenience this situation may cause; if you have questions, please feel free to call (866) 983-9384, Monday through Friday from 8:00 a.m. to 9:00 p.m. Eastern Time and Saturday from 8:00 a.m. to 3:00 p.m. Eastern Time (excluding major bank holidays).

Sincerely,

LoanCare, LLC

Description of Monitoring Services

You have been provided with access to the following services:

KROLL

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some you may consider:

Reviewing Your Accounts and Credit Reports

Regulators recommend that you be especially vigilant for the next 12 to 24 months and that you promptly report incidents of suspected identity theft to your financial institution. As part of staying vigilant, you should regularly review your account statements, and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

Equifax	**Experian**	**TransUnion**
1-800-525-6285	1-888-397-3742	1-800-680-7289
Equifax.com	Experian.com	Transunion.com
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

You can obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report by calling toll free 1-877-322- 8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert

A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report

A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will provide you a PIN number or a password when you place a security freeze. You will need that PIN or password to lift the freeze, and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft

If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

File a Police Report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and file a complaint online at www.IdentityTheft.gov. You can also file a complaint by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of *Identity Theft: A Recovery Plan*, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Special Information for Residents of the District of Columbia, Iowa, Maryland, Massachusetts, New Mexico, New York, North Carolina, Oregon, Rhode Island, and Vermont.-

District of Columbia residents can learn more about preventing identity theft from the District of Columbia Office of the Attorney General, by visiting their website at https://oag.dc.gov, calling 1.202.727.3400, or requesting more information via email oag@dc.gov or mail 400 6th Street NW, Washington DC 20001.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling 1.515.281.5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at http://www.marylandattorneygeneral.gov, calling the Identity Theft Unit at 1.410.576.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to its honoring your request.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above.

New York residents may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 1.800.771.7755.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at https://ncdoj.gov/protecting-consumers/protecting-your-identity; calling 1.919.716.6400, 1.877.566.7226, or 1.919.716.6000; or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling 1.503.378.4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096. You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by visiting the website at https://riag.ri.gov, by phone at 1.401.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at https://ago.vermont.gov/cap/scam-prevention-through-awareness-and-education/identity-theft