**THE UNITED STATES DISTRICT COURT**

**FOR THE DISTRICT OF NEW JERSEY**

| | |
|---|---|
| MATTHEW STUART, as an individual and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>AMERICAN FINANCIAL RESOURCES, INC.,<br><br>Defendant. | Case No.:<br><br>**CLASS ACTION COMPLAINT**<br><br>DEMAND FOR JURY TRIAL |

Plaintiff Matthew Stuart ("Plaintiff") brings this Class Action Complaint against American Financial Resources, Inc. ("AFR" or "Defendant"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

## INTRODUCTION

1. Plaintiff brings this class action against AFR to seek damages for Plaintiff and the class of consumers and current or former employees of AFR who he seeks to represent, as well as other equitable relief, including, without limitation, injunctive relief designed to protect the very sensitive information of Plaintiff, other consumers, and current or former AFR employees. This action arises from AFR's failure to properly secure and safeguard personal identifiable information, including without limitation, the names, Social Security numbers, driver's license or state-issued identification numbers, and account numbers (collectively, "Sensitive Information" or "PII").

2. AFR is a mortgage lending company that provides real estate lending services to thousands of mortgage brokers, bankers, lenders, homeowners, home buyers, realtors, and contractors across the country.

3. As part of its services, AFR requires that its customers, including Plaintiff and Class Members, provide AFR with their PII, including name, social security number, and driver's license information.

4. Beginning on or about March 9, 2022, AFR notified state Attorneys General and/or many of its customers about a widespread data breach involving sensitive PII of thousands of individuals, including customers and current or former employees.[1] As an example, AFR notified the New Hampshire Attorney General on March 11, 2022 that there were 954 Massachusetts residents affected by the breach.[2] AFR similarly notified the Washington Attorney General on March 11, 2022 that there were 6,570 Washington residents impacted by the breach, including current or former employees of AFR.[3] AFR explained its investigation concluded on February 4, 2022 that between December 6-20, 2021, AFR allowed its network to be "accessed without authorization" by unknown third parties, exposing and allowing access to and acquisition of the PII for individual customers detailed above ("Data Breach").[4]

5. The full extent of the types of sensitive personal information, the scope of the breach, and the root cause of the Data Breach is all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors at this phase of litigation.

---

[1] Ex. 1, March 9, 2022 letter from William S. Packer, Executive Vice President and Chief Operations Officers of AFR to Matthew Stuart ("March 9, 2022 Letter").
[2] https://www.doj.nh.gov/consumer/security-breaches/documents/american-financial-resources-20220311.pdf (last visited March 22, 2022).
[3] https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachM13162.pdf (last visited March 22, 2022).
[4] March 9, 2022 Letter.

6. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and Class Members, to keep their PII confidential, safe, secure, and protected from unauthorized disclosure or access.

7. Moreover, by obtaining, collecting, using, and deriving benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to those persons, and knew or should have known that it was responsible for safeguarding and protecting Plaintiff's and Class Members' PII from unauthorized disclosure or criminal hacking activity.

8. In acquiring and maintaining Plaintiff's and Class Members' Sensitive Information, Defendant expressly and impliedly promised to safeguard Plaintiff's and Class Members' PII.

9. Plaintiff and Class Members reasonably expected and relied upon Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

10. Plaintiff and Class Members would not have paid the amounts they paid for Defendant's services, had they known their information would be maintained using inadequate data security systems. Defendant, however, breached their duties, promises, and obligations, and Defendants' failures increased the risk that Plaintiff's Sensitive Information would be compromised in the event of a likely cyberattack.

11. Upon information and belief, Defendant is responsible for allowing this Data Breach because of multiple acts of negligence, including but not limited to its: failure to design, implement, and maintain reasonable data security systems and safeguards; and/or failure to exercise reasonable care in the hiring, supervision, and training of its employees and agents and

vendors; and/or failure to comply with industry-standard data security practices; and/or failure to comply with federal and state laws and regulations that govern data security and privacy practices and are intended to protect the type of Sensitive Information at issue in this action.

12. Upon information and belief, despite its role in managing so much Sensitive Information, Defendant failed to take basic security measures such as encrypting its data or following industry security standards. Moreover, Defendant failed to recognize and detect that unauthorized third parties had accessed its network. Defendant further failed to recognize that substantial amounts of data had been compromised, and more likely than not, exfiltrated and stolen. Had Defendant not committed the acts of negligence described herein, it would have discovered the Data Breach sooner – and/or prevented the invasion and theft altogether.

13. In this era of frequent data security attacks and data breaches, particularly in the financial industry, Defendant's failures leading to the Data Breach are particularly egregious, as this Data Breach was highly foreseeable.

14. And as a result of Defendant's failures to protect the PII of Plaintiff and Class Members the PII was compromised and accessed. Upon information and belief, their Sensitive Information was likely downloaded, and/or exfiltrated by malicious cyber criminals, who targeted that information through their wrongdoing.

15. Criminal hackers obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members.

16. As a direct and proximate result of the Data Breach, Plaintiff and the Class Members are now at a significant present and future risk of identity theft, financial fraud and/or other identity-theft or fraud, imminently and for years to come.

17. In the months and years following the Data Breach, Plaintiff and the other Class Members will experience numerous types of harms as a result of Defendant's ineffective and inadequate data security measures. Some of these harms will likely include fraudulent charges on financial accounts, opening fraudulent financial accounts, and targeted advertising without patient consent.

18. Plaintiff and Class Members have also now lost the economic value of their Sensitive Information. Indeed, there is both a healthy black market and a legitimate market for that PII. Just as Plaintiff's and Class Members' PII were stolen, *inter alia*, because of its inherent value in the black market, the inherent value of Plaintiffs' and the Class Members' Sensitive Information in the legitimate market is now significantly and materially decreased.

19. Plaintiff and Class Members have suffered numerous actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their Sensitive Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) invasion of privacy; (e) emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) the diminution in value of their personal data; (h) the loss of value of the bargain for paying for services that required entrusting their Sensitive Information to Defendant with the mutual understanding that Defendant would safeguard the Sensitive Information against improper disclosure, misuse, and theft; and (h) the continued risk to their Sensitive Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as

Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Sensitive Information.

20. Plaintiff seeks to remedy these harms, and to prevent their future occurrence, on behalf of themselves and all similarly situated persons whose Sensitive Information were compromised as a result of the Data Breach.

21. Accordingly, Plaintiff, on behalf of himself and other Class Members, asserts claims for negligence (Count I); negligence *per se* (Count II); breach of fiduciary duty (Count III); breach of implied contract (Count IV); and Declaratory Judgment (Count V).

## PARTIES

***Plaintiff Mathew Stuart***

22. Plaintiff Matthew Stuart is a resident and citizen of Illinois residing in Cook County, Illinois. Mr. Stuart received AFR's Notice of Data Breach, dated March 9, 2022, shortly after that date.

23. The letter, dated March 9, 2022, informed Plaintiff Stuart that, following an internal investigation, Defendant had determined that certain AFR files were accessed without authorization between December 6th and December 20th, 2021. The letter further state that a comprehensive review concluded that compromised files contained Plaintiff Stuart's name, Social Security Number, and potentially his Driver's license number.

***Defendant AFR***

24. Defendant AFR is a New Jersey corporation with its principal place of business at 9 Sylvan Way, Parsippany, NJ 07054.

25. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

26. All of Plaintiff's claims stated herein are asserted against AFR and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

## JURISDICTION AND VENUE

27. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member (including, for example, named Plaintiff Matthew Stuart, a citizen of Illinois) is a citizen of a state different from Defendant ( a citizen of New Jersey) to establish minimal diversity.

28. The District of New Jersey has personal jurisdiction over Defendant named in this action because Defendant is incorporated and has its principal place of business in this District, conducts substantial business in this District through its headquarters, offices, and affiliates, and (upon information and belief) engaged in the conduct at issue here in this judicial district.

29. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered and has its principal place of business in this District and has caused harm to Plaintiff and Class Members through conduct in this District.

## FACTUAL ALLEGATIONS

***Background***

30. AFR promises that it will protect its customers' privacy and remain in compliance with statutory privacy requirements. For example, AFR states in its Privacy Statement (last updated February 1, 2021) posted on its website that:

> American Financial Resources, Inc. (herein referred to as AFR) has been committed to your financial well-being and protecting the privacy and security of the information you share with us since our inception in 1997.
>
> This Privacy Disclosure Statement applies to your interaction with American Financial Resources, Inc or any of its wholly-owned subsidiaries or brands, including, but not limited to AFR, AFR Wholesale, eLEND and Manufactured Home.Loan. including any online or mobile site or application that we own and/or control ("Site"), unless a different online and/or mobile policy is posted at a particular site, or is made available to you and by its terms supplants this Policy.[5]

31. AFR also promises consumers that "Social Security numbers are classified as 'Confidential' information under the AFR Information Security Policy. As such, Social Security numbers may only be accessed by and disclosed to AFR employees and others with a legitimate business 'need to know' in accordance with applicable laws and regulations."[6]

32. Plaintiff and the Class Members, as current and former AFR customers, and/or current and former AFR employees, relied on these expressed and implied promises and on this sophisticated entity to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Consumers, in general, demand security to safeguard their PII, especially when Social Security numbers and other sensitive PII is involved.

[5] Ex. 2, https://www.afrcorp.com/privacy-statement/ (last visited March 22, 2022).
[6] *Id.*

33. AFR had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

***The Data Breach***

34. Beginning on or about March 9, 2022, AFR notified many of its customers, current and former employees, and state Attorneys General about a widespread data breach involving sensitive PII of certain current and former customers.

35. Through an investigation, AFR determined that the unauthorized individual or individuals had access to its systems between December 6 and 20, 2021 (i.e. unauthorized access over fourteen (14) calendar days).[7] This exposed at least thousands of consumers' PII to criminals.

36. On February 4, 2022, an investigation commissioned by AFR determined that there was unauthorized activity on AFR's network that resulted in unauthorized third-party access to and acquisition of confidential information of AFR customers.[8]

37. The confidential information that was accessed without authorization included names along with data elements including Social Security numbers, account numbers, "and for some individuals, driver's license number[s]."[9]

38. Upon information and belief, the PII was not encrypted prior to the data breach.

39. Upon information and belief, the cyberattack was targeted at AFR due to its status as a major real estate mortgage company that collects valuable personal and financial data on its many customers, as well as its employees.

[7] March 9, 2022 Letter.
[8] *Id.*
[9] *Id.*

40. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiff and the Class Members.

41. On or about March 9, 2022, AFR sent customers (including Mr. Stuart) and current or former employees a Notice of Data Breach, informing the recipients of the notice that their confidential data was involved, and stating:

> We wanted to notify you of the incident and assure you that we take it very seriously. We also encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. If you see charges or activity you did not authorize, please contact your financial institutions immediately.
>
> Additionally, AFR is offering you a complimentary one-year membership to Kroll's identity monitoring services. This service helps detect possible misuse of your personal information and provides you with identity monitoring services focused on immediate identification and resolution of identity theft. . . .
>
> To help prevent something like this from happening in the future, we have implemented additional measures to enhance our existing security protocols. These measures include deploying a new advanced endpoint detection and response tool, resetting user passwords, upgrading server and domain controller software, and enhancing multifactor authentication.[10]

42. AFR admitted in the Notice of Data Breach and the letters to the Attorneys General that their systems were subjected to unauthorized access beginning on or about December 6-20, 2021, and there is no indication that the exfiltrated PII was retrieved from the cybercriminals who took it.[11]

43. AFR's offer of credit and identity monitoring services, AFR's suggestion to "remain vigilant," as well as the express warning for any "unauthorized activity" is an

[10] *Id.*
[11] *Id.*, *see also* fn. 2-4.

acknowledgment by AFR that the impacted customers are subject to an imminent threat of identity theft and financial fraud.

44. In response to the Data Breach, AFR claims, "we implemented additional measures to further enhance our security protocols." AFR further admits that enhanced "security protocols" were required, but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' PII going forward.[12]

45. AFR had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their PII confidential and to protect it from unauthorized access and disclosure.

46. Plaintiff and Class Members provided their PII to AFR with the reasonable expectation and mutual understanding that AFR would comply with its obligations and representations to keep such information confidential and secure from unauthorized access.

47. AFR failed to uphold its obligations to Plaintiff and Members of the Class. As a result, Plaintiff and Class Members have been significantly harmed and will be at a high risk of identity theft and financial fraud for many years to come.

48. AFR did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining, causing Plaintiff's and Class Members' PII to be exposed.

***Securing PII and Preventing Breaches***

49. AFR could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and computer files containing PII.

[12] *Id.*

50. AFR has acknowledged the sensitive and confidential nature of the PII. To be sure, collecting, maintaining, and protecting PII is vital to many of AFR's business purposes. AFR has acknowledged through conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

***The Data Breach Was a Foreseeable Risk of which Defendant Was on Notice***

51. It is well known that PII, including social security numbers and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

52. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.

53. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being exposed exceeding 100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.

54. The 108 reported financial sector data breaches reported in 2019 exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.

55. Consumers place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

56. Consumers are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers." There are long-term consequences to data breach victims whose social

security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."

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

58. 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 prepared for, a potential attack.

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

***At All Relevant Times, AFR Had a Duty to Plaintiff and Class Members to Properly Secure their Private Information***

60. At all relevant times, AFR had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly notify Plaintiff and Class Members when AFR became aware that their PII may have been compromised.

61. AFR's duty to use reasonable security measures arose as a result of the special relationship that existed between AFR, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class entrusted AFR with their PII when they purchased financial products or services from AFR.

62. AFR had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, AFR breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

63. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

64. 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."

65. The ramifications of AFR's failure to keep its consumers' PII secure are long-lasting and severe. Once PII is stolen, particularly Social Security and driver's license numbers, fraudulent use of that information and damage to victims may continue for years.

***The Value of Personal Identifiable Information***

66. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[13] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[14] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

---

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

[14] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, available at: https://www.privacyaffairs.com/dark-web-price-index-2021/

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

67. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as 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 assuming your identity can cause a lot of problems.[16]

68. 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.

69. Even then, a new 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."[17]

70. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card

[16] Social Security Administration, Identity *Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.
[17] 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.

information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[18]

71. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[19]

72. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you.
>
> Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[20]

73. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[21] However, this is not the case. As cybersecurity experts point out:

---

[18] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[19] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last accessed November 2, 2021)

[20] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?* (October 24, 2018) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last accessed November 2, 2021)

[21] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed November 2, 2021)

> It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.[22]

74. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[23]

75. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[24]

76. Given the nature of the Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Class Members' PII can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

77. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts.[25] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

---

[22] *Id.*
[23] *How Identity Thieves Took My Wife for a Ride*, NY Times, April 27, 2021 https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed November 2, 2021)
[24] See OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.
[25] See Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, *Forbes*, Mar 25, 2020, available at: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

78. To date, AFR has offered its consumers only one year of identity monitoring service. The offered services are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

79. The injuries to Plaintiff and Class Members were directly and proximately caused by AFR's failure to implement or maintain adequate data security measures for its current and former customers.

***AFR Failed to Comply with FTC Guidelines***

80. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[26]

81. 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.[27] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

[26] Federal Trade Commission, *Start With Security*, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[27] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

82. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[28]

83. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.
b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.
c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.
d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.
e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks
f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.
g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.
h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.
i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

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

[28] FTC, Start With Security, supra note 28.

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.

85. Because Class Members entrusted AFR with their PII, AFR had, and has, a duty to the Class Members to keep their PII secure.

86. Plaintiff and the other Class Members reasonably expected that when they provide PII to AFR, AFR would safeguard their PII.

87. AFR was at all times fully aware of its obligation to protect the personal and financial data of consumers, including Plaintiff and members of the Classes. AFR was also aware of the significant repercussions if it failed to do so.

88. AFR's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiff's and Class Members' Social Security numbers, driver's license numbers, financial/payment card information, and other highly sensitive and confidential information— constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

***Plaintiff and Class Members Have Suffered Concrete Injury As A Result Of Defendant's Inadequate Security And The Data Breach It Allowed***

89. Plaintiff and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information, including their Social Security numbers and driver's license numbers.

90. Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for its service, Plaintiff and other reasonable consumers understood and expected that they were paying for services and data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class

Members received services that were of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

91. Cybercriminals capture PII to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened risk of identity theft. Plaintiff has also incurred (and will continue to incur) damages in the form of, inter alia, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

92. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

a. obtaining employment;
b. obtaining a loan;
c. applying for credit cards or spending money;
d. filing false tax returns;
e. stealing Social Security and other government benefits; and
f. applying for a driver's license, birth certificate, or other public document.

93. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

94. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

95. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.[29]

96. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[30] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[31] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[32] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

97. As a result of the Data Breach, Plaintiff and Class Members have already suffered damages.

98. Since the Data Breath, Defendant has represented to the Class Members that a "comprehensive review" reveals that customers' individual files were accessed. Regardless, EmiSoft, an award-winning malware-protection software company, states that "[a]n absence of

---

[29] *Id.*
[30] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267.
[31] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php.
[32] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH-IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (available at https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf).

evidence of exfiltration should not be construed to be evidence of its absence, especially during the preliminary stages of the investigation."[33]

99. In this case, according to AFR, cybercriminals had access to Plaintiff and Class Members' data on at least December 6, 2021 to December 20, 2021.

100. However, even if AFR has not found evidence of data being exfiltrated and viewed, this would not be an assurance that the data was not accessed, acquired, and stolen. Indeed, the likelihood that cybercriminals stole the data covertly is significant, likely, and concerning.

***Plaintiff Stuart's Experience***

101. In or about early 2021, Plaintiff Stuart was a former AFR customer using the service on a previous home mortgage. As a condition to receiving the services, AFR required Plaintiff to to supply, and he provided, AFR with his PII, including but not limited to his name, address, date of birth, Social Security number, driver's license number, telephone number and email address, to participate in AFR's services. Upon information and belief, at the time of engaging the services, Plaintiff's PII was entered into AFR systems.

102. Plaintiff Stuart greatly values his privacy and Sensitive Information, especially when receiving loan and financial services. Plaintiff has taken reasonable steps to maintain the confidentiality of his PII, and he has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

103. Plaintiff Stuart expected and reasonably relied upon Defendant as part of its services to provide adequate data security to protect the PII that he entrusted to Defendant. If Mr.

[33] EmiSoft Malware Lab, The chance of data being stolen in a ransomware attack is greater than one in ten (EMISOFT BLOG July 13, 2020), https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/.

Stuart had known that AFR would not adequately protect his PII, he would not have allowed AFR access to this sensitive and private information, and would not have engaged in business with Defendant.

104. Upon information and belief, Plaintiff's PII was targeted, accessed, and downloaded and stolen by the third-party criminal actors in the Data Breach.

105. As a result of the Data Breach, Plaintiff Stuart faces a substantial risk of imminent identity, financial, and health fraud and theft—both now and for years to come. Mr. Stuart has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

106. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Stuart faces, Defendant provided Plaintiff Stuart a one-year subscription to a credit monitoring service. However, Plaintiff Stuart has not sign up for the program, as he already has credit monitoring services from unrelated sources.

107. As a result of the Data Breach, Mr. Stuart suffered actual injury and damages in paying money to AFR for identity services before the Data Breach; expenditures which he would not have made had AFR disclosed that it lacked data security practices adequate to safeguard PII.

108. Mr. Stuart also suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that he entrusted to AFR for the purpose of providing him services, which was compromised in and as a result of the Data Breach.

109. Furthermore, Mr. Stuart suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number.

110. Moving forward, Mr. Stuart has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in AFR's possession, is protected and safeguarded from future breaches.

## CLASS ALLEGATIONS

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

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

> **All persons who reside in the United States who received or were otherwise sent the AFR notice that their data was potentially compromised due to the Data Breach.**

113. The above class and subclasses are herein referred to as the "Classes."

114. Excluded from the Classes are the following individuals and/or entities: AFR and AFR's parents, subsidiaries, affiliates, officers and directors, and any entity in which AFR has 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.

115. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

116. Numerosity, Fed R. Civ. P. 23(a)(1): Classes are so numerous that joinder of all members is impracticable. AFR has identified over 3,100 consumers whose PII may have been

improperly accessed in the Data Breach, and the Classes are apparently identifiable within AFR's records.

117. 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 AFR had a duty to protect the PII of Plaintiff and Class Members;

b. Whether AFR had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

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

d. Whether AFR expressly or impliedly promised to safeguard the PII of Plaintiff and Class Members.

e. Whether AFR failed to adequately safeguard the PII of Plaintiff and Class Members;

f. Whether and when AFR actually learned of the Data Breach;

g. Whether AFR adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

h. Whether AFR violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

i. Whether AFR failed to design, implement and maintain reasonable security procedures and practices in compliance with industry standards and appropriate to the nature and scope of the information compromised in the Data Breach;

j. Whether AFR adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

k. Whether AFR engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

l. Whether Plaintiff and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of AFR's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of AFR's wrongful conduct;

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

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

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

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

121. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the

controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like AFR. 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.

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

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

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

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

126. Further, AFR has acted or refused to act on grounds generally applicable to the Class 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.

127. 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 AFR owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

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

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

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

e. Whether AFR breached the implied contract;

f. Whether AFR adequately, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether AFR 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 AFR engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual damages, statutory damages, injunctive relief, and/or punitive damages as a result of AFR's wrongful conduct

**COUNT I**
**Negligence**

**(On behalf of Plaintiffs and the Nationwide Class)**

128. Plaintiff restates and realleges all of the foregoing Paragraphs 1 through 127 as if fully set forth herein.

129. As a condition of their using the services of AFR, consumers were obligated to provide AFR with certain PII, including their name, date of birth, address, Social Security number, driver's license, telephone number, email address, financial account numbers, and payment card numbers.

130. Plaintiff and Class Members entrusted their PII to AFR on the premise and with the understanding that AFR would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

131. AFR has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

132. AFR knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their consumers' PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

133. AFR 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 AFR's security protocols to ensure that Plaintiff's and Class Members' information in AFR's possession was adequately secured and protected.

134. AFR also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

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

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

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

138. Plaintiff and the Class Members had no ability to protect their PII that was in, and possibly remains in, AFR's possession.

139. AFR was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

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

141. AFR had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

142. AFR has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

143. AFR, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII was within AFR's possession or control.

144. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

145. These foregoing frameworks are existing and applicable industry standards in the financial services industry, and Defendant failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

146. AFR improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

147. AFR failed to heed industry warnings and alerts to provide adequate safeguards to protect consumers' PII in the face of increased risk of theft.

148. AFR, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its consumers' PII.

149. AFR, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

150. But for AFR's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

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

152. As a direct and proximate result of AFR's negligence, Plaintiff and Class Members 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 actual and future 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 AFR's possession and is subject to further unauthorized disclosures so long as AFR fails to undertake

appropriate and adequate measures to protect the PII of consumers in their continued possession; (viii) 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 Class Members; and (ix) the diminished value of AFR's goods and services they received.

153. As a direct and proximate result of AFR's negligence, Plaintiff and Class Members 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.

154. Additionally, as a direct and proximate result of AFR's negligence and negligence per se, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in AFR's possession and is subject to further unauthorized disclosures so long as AFR fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

**COUNT II**
**Negligence Per Se**

**(On behalf of Plaintiffs and the Nationwide Class)**

155. Plaintiff restates and realleges the foregoing Paragraphs 1 through 154 as if fully set forth herein.

156. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiff and Class Members.

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

158. Pursuant to the Gramm-Leach-Bliley Act, Defendant had a duty to protect the security and confidentiality of Plaintiff's and Class Members' PII. *See* 15 U.S.C. § 6801.

159. Pursuant to the Fair Credit Reporting Act ("FCRA"), Defendant had a duty to adopt, implement, and maintain adequate procedures to protect the security and confidentiality of Plaintiff's and Class Members' PII. *See* 15 U.S.C. § 1681(b).

160. Defendant solicited, gathered, and stored PII of Plaintiff and the Class Members to facilitate transactions which affect commerce.

161. Defendant violated the FTC Act (and similar state statutes), FCRA, and the Graham-Leach-Bliley Act by failing to use reasonable measures to protect PII of Plaintiff and Class Members and not complying with applicable industry standards, as described herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

162. Defendant's violation of the FTC Act (and similar state statutes) as well as its violations of the FCRA, and the Graham-Leach-Bliley Act constitutes negligence per se.

163. Plaintiff and the Class Members are within the class of persons that the FTC Act (and similar state statutes), the FCRA, and the Graham-Leach-Bliley Act were intended to protect.

164. The harm that occurred as a result of the breach is the type of harm the FTC Act (and similar state statutes), as well as the FCRA, and the Graham-Leach-Bliley Act were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures caused the same harm as that suffered by Plaintiff and the Class Members.

165. As a direct and proximate result of Defendant's negligence per se, Plaintiff and Class Members have suffered, and continue to suffer, damages arising from the breach as described herein and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

166. As a direct and proximate result of Defendant's negligence per se and the data breach, Plaintiff and members of the proposed Class 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 Defendant promised when Plaintiff and the proposed class entrusted Defendant with their PII; and (h) the continued and substantial risk to Plaintiff and Class Members PII, which remains in the Defendant's possession of Defendant with in-adequate measures to protect Plaintiff's and Class Members' PII.

## COUNT III
## Breach of Fiduciary Duty

**(On behalf of Plaintiffs and the Nationwide Class)**

167. Plaintiff restates and realleges the foregoing Paragraphs 1 through 166 as if fully set forth herein.

168. In providing their Sensitive Information to Defendant, Plaintiffs and Class Members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiff and Class Members to safeguard and keep confidential that Sensitive Information.

169. Defendant accepted the special confidence Plaintiffs and Class Members placed in it, as evidenced by its assertion that it is "committed to protecting the privacy of [Plaintiff's] personal information" as included in the Data Breach notification letters.

170. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became a guardian of Plaintiff's and Class Members' Sensitive Information, Defendant became a fiduciary by its undertaking and guardianship of the Sensitive Information, to act primarily for the benefit of its customers, including Plaintiff and Class Members for the safeguarding of Plaintiff' and Class Members' Sensitive Information.

171. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its customer's relationship, in particular, to keep secure the Sensitive Information of its customers.

172. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to protect the integrity of the systems containing Plaintiff's and Class Members' Sensitive Information.

173. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Sensitive Information.

174. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their Private Information; (c)

out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Cyber-Attack and Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Cyber-Attack and Data Breach for the remainder of the lives of Plaintiff and Class Members; and (g) the diminished value of Defendant's services they received.

175. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

## COUNT IV
## Breach of Implied Contract
## (On behalf of Plaintiffs and the Nationwide Class)

176. Plaintiff restates and realleges the foregoing Paragraphs 1 through 175 as if fully set forth herein.

177. As a condition of receiving services, Defendant required Plaintiff and Class Members to provide their PII, including names, Social Security numbers, driver's license numbers, addresses, dates of birth, email addresses, financial account numbers, and payment card numbers.

178. Defendant solicited and invited Plaintiff and Class Members to provide their Private Information as part of Defendant's regular business practices.

179. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant. Defendant accepted the PII, and there was a meeting of the minds that Defendant would secure, protect, and keep the PII confidential.

180. Plaintiff fully performed his obligations under the implied contracts with Defendant.

181. Plaintiff would not have entered into transactions with AFR if Plaintiff had known AFR would not protect their PII.

182. When AFR required and accepted the PII from Plaintiff and the Class, it implied its assent to protect the information sufficiently.

183. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their PII, and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

184. Plaintiff and Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

185. As a direct and proximate result of Defendant's above-described breach of implied contract, have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity how their PII is used; (c) the compromise, publication, and/or theft of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (e) 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 tax fraud and identity theft; (f) costs associated with placing freezes on credit reports; (g) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of consumers and former consumers in its continued possession; (h) 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 Class Members; and (i) the diminished value of AFR's goods and services they received.

186. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

187. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) immediately provide adequate credit monitoring to all Class Members.

## COUNT V
## Declaratory Judgment

**(On behalf of Plaintiffs and the Nationwide Class)**

188. Plaintiff restates and realleges all of the foregoing paragraphs as if fully set forth herein.

189. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

190. Plaintiff and Class Members entered into an implied contract that required Defendant to provide adequate security for the PII it collected from Plaintiff and Class Members.

191. Defendant owes a duty of care to Plaintiff and Class Members requiring them to adequately secure PII.

192. Defendant still possesses PII regarding Plaintiff and Class Members.

193. Since the Data Breach, Defendant has announced few if any specific and significant changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent further attacks.

194. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

195. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

196. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

197. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Defendant

must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage 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 Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant not transmit PII via unencrypted email;

f. Ordering that Defendant not store PII in email accounts;

g. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

h. Ordering that Defendant conduct regular computer system scanning and security checks;

i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendant to meaningfully educate their current, former, and prospective customers about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiff, on behalf of himself and all Class Members, requests judgment against the AFR and that the Court grant the following:

A. For an Order certifying the Nationwide Class and appointing Plaintiff and their Counsel to represent the certified Class;

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

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

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

ii. requiring AFR 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 AFR to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless AFR can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring AFR to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' personal identifying information;

v. prohibiting AFR from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring AFR 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 AFR's systems on a periodic basis, and ordering AFR to promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

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

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

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

xiii. requiring AFR 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 AFR's policies, programs, and systems for protecting personal identifying information;

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

xv. requiring AFR 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 AFR to implement logging and monitoring programs sufficient to track traffic to and from AFR's servers; and

xvii. 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 AFR's 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; and

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

E. For an award of punitive damages;

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

G. For prejudgment interest on all amounts awarded; and

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

**DEMAND FOR JURY TRIAL**

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

Dated: April, 1, 2022

Respectfully Submitted,

THE LAW OFFICES
JOSEPH D. MONACO, P.C.

By: *Joseph D. Monaco, Esq.*
Joseph D. Monaco, III
7 Penn Plaza - Suite 1606
New York, New York 10001
(212) 486-4244
jmonaco@monaco-law.com

Joseph M. Lyon (*Pro Hac Vice forthcoming*)
THE LYON FIRM, LLC
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 721-1178
jlyon@thelyonfirm.com

Terence R. Coates (*Pro Hac Vice forthcoming*)
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

***Counsel for Plaintiff and the Class***