IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

ARTUR PODROYKIN, *on behalf of himself and all individuals similarly situated,* Plaintiffs, v. AMERICAN ARMED FORCES MUTUAL AID ASSOCIATION, Defendant.	Civil Action No. 1:21-cv-588

CLASS ACTION COMPLAINT

Plaintiff Artur Podroykin ("Plaintiff" or "Mr. Podroykin"), individually and on behalf of all other persons similarly situated, and through his attorneys of record, alleges the following against Defendant American Armed Forces Mutual Aid Association ("Defendant" or "AAFMAA") based on personal knowledge with respect to himself, on information and belief derived from investigation of counsel, and review of public documents as to all other matters.

INTRODUCTION

1. Mr. Podroykin is a service-disabled veteran of the United States Army and a member of the AAFMAA, a mutual aid association for active duty members and veterans of the United States military, along with their families. AAFMAA sells its members life insurance policies, mortgage services, financial planning, and other services.

2. While purchasing a life insurance policy through AAFMAA in 2010, Mr. Podroykin was required to provide AAFMAA with a litany of personally identifiable information ("PII"), including protected health information ("PHI"), as discussed further below.

3. Unfortunately for Mr. Podroykin and his fellow members of AAFMAA, Defendant did not adequately safeguard their data, and Mr. Podroykin and tens of thousands of other military veterans are now the victims of a large-scale data breach that will impact them for years to come.

4. On January 29, 2021, AAFMAA became aware of suspicious activity on its computer systems and "determined that an unauthorized actor gained access to certain AAFMAA systems between January 2, 2021 and January 31, 2021 and removed and/or viewed certain files from [AAFMAA's] network" (the "Breach" or "Data Breach").[1]

5. It was not until on or about March 5, 2021, that AAFMAA sent a Notice of Data Breach to its affected members, including Mr. Podroykin (the "Notice"). The Notice informed Mr. Podroykin that his PII had been compromised in the Data Breach; specifically, his name and Social Security number.

6. The Notice of Data Breach did not disclose that additional treasure troves of PII/PHI were stored on AAFMAA's servers, and thus Mr. Podroykin cannot be sure that even more of his PII/PHI was not compromised in the Data Breach.

7. AAFMAA is responsible for allowing the Data Breach to occur because it failed to implement and maintain any reasonable safeguards and failed to comply with industry-standard data security practices, contrary to the representations made in AAFMAA's privacy statements.

8. Because of AAFMAA's failure to exercise due care, Mr. Podroykin and the Class Members have been injured through the loss of control of their PII/PHI, the diminished value of their PII/PHI, the need to spend time to take appropriate steps to mitigate their injuries, and the actual, heightened, and/or imminent risk of identity theft or fraud.

PARTIES

Plaintiff

9. Mr. Podroykin is an adult who resides in and is a citizen of Champaign, Illinois.

[1] *See* https://media.dojmt.gov/wp-content/uploads/aafSamp.pdf (last visited April 15, 2021)

10. Mr. Podroykin obtained a life insurance policy from AAFMAA in 2010. In applying for the life insurance policy, Mr. Podroykin provided AAFMAA with at least the following PII: his name, date of birth, social security number, age, address, email address, copy of his driver's license, credit card information, as well as PHI—including specific information regarding his medical history (by completing a medical questionnaire provided by AAFMAA).

11. On or about March 5, 2021, Mr. Podroykin received the Notice from AAFMAA confirming the Data Breach, and noting that his name and Social Security Number had been compromised.[2]

12. Mr. Podroykin's PII (including at least his name and Social Security number, as disclosed in the Notice) was compromised in the Data Breach. As set forth below, Mr. Podroykin has every reason to believe that his other PII, including his PHI, was also compromised in the Breach.

13. As a result of Mr. Podroykin's data being compromised in the Data Breach, Mr. Podroykin has spent approximately twenty-one hours checking his account statements to monitor for any instances of financial fraud or identity theft. It took Mr. Podroykin this much time, in part, because he suffers from certain cognitive issues arising from his service-related disability. Due to his reasonable fear of identity theft following the Breach, and as a direct result of learning of the Breach, Mr. Podroykin also purchased a shredder to destroy documents that potentially contain PII or other information that could be used by identity thieves in combination with the PII compromised in the Breach, as well as an ink roller to render unreadable such PII or other information on letters he receives in the mail.

14. Additionally, upon receiving the Notice, Mr. Podroykin experienced significant emotional distress because of his reasonable belief that his PII (and, potentially, his PHI) is now in the hands of unauthorized third parties, and as a result, he faces an impending and heightened risk of identity theft and fraud. This is the only time Mr. Podroykin recalls receiving a Notice of Data Breach in the mail. He originally thought the letter was just another solicitation for a life insurance policy.

[2] A true and correct copy of the Notice sent to Mr. Podroykin is attached hereto as **Exhibit A.**

When he read the letter, including AAFMAA's offer of Experian credit monitoring services, he knew that his identity was in jeopardy. Mr. Podroykin experienced heightened anxiety and depression upon learning of the Data Breach, to the point where he had to sit down as his hands were shaking. He continues to experience emotional distress arising from the fear that his PII (and, potentially, his PHI) will be misused. This is compounded by the fact that AAFMAA is in possession of his minor child's PII (however, AAFMAA has not disclosed whether Mr. Podroykin's child's PII was compromised in the Breach).

15. Mr. Podroykin has not previously been subject to identity theft, and he is not aware of any prior compromise of his Social Security number in a prior data breach incident. As a consumer concerned with data theft, data breaches, and criminal activity, Mr. Podroykin has taken considerable steps to protect his identity and maintain his privacy prior to the Data Breach and since the Data Breach. Mr. Podroykin has refrained from transmitting unencrypted PII over the internet or any other unsecured source. Mr. Podroykin also stores any and all documents containing his PII in a safe and secure physical location, and destroys any documents he receives in the mail that contain his PII or that might contain information that could otherwise be used to steal his identity (including, before the Breach, by tearing up junk mail into small pieces and bringing any documents containing PII/PHI to UPS to be shredded; he now uses the shredder he bought following the Breach).

Defendant

16. AAFMAA is a Virginia not-for-profit corporation with its principal place of business in Fort Meyer, Virginia. AAFMAA sells its members life insurance policies, mortgage services, financial planning, and other services. AAFMA is not affiliated with the United States government or the United States military.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative Class Members, and minimal diversity

exists because Mr. Podroykin and many putative Class Members are citizens of a different state than AAFMA.

18. This Court has personal jurisdiction over AAFMAA because it is authorized to and regularly conducts business in Virginia, and is headquartered in Fort Meyer, Virginia.

19. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Mr. Podroykin's claims occurred in this District.

FACTUAL ALLEGATIONS

AAFMAA and Its Privacy and Data Security Representations

20. AAFMAA collects the PII/PHI of tens of thousands of its members when they apply to receive life insurance, mortgage services, financial advisory services, and other services from AAFMAA.

21. AAFMAA is fully aware of the sensitive nature of its members' PII/PHI that it collects, admitting in its Online Privacy Policy that it collects at least the following PII/PHI: "[The member's] name, mailing address, phone number, email address, birth date, Social Security Number, passport number, driver's license number, military records, payment information, financial information (such as assets, income, account balances), health information, and similar information relating to [the member's] spouse and children."[3]

22. AAFMAA represents to its customers through the Online Privacy Policy that it will "[m]aintain, monitor and update physical, electronic and procedural safeguards to protect personal information," "[u]se security and encryption methods to help prevent data breaches and unauthorized disclosure of personal information," "[r]estrict access to personal information to necessary personnel only," and "make commercially reasonable efforts to handle such information consistent with this Privacy Policy and applicable laws."[4]

[3] *See* https://www.aafmaa.com/about/privacy-policy (last visited April 15, 2021).
[4] *Id.*

23. AAFMAA's Online Privacy Policy also details the limited scenarios in which it will share its members' PII/PHI. Of course, those limited scenarios do not include sharing PII/PHI with unauthorized third parties, and certainly not criminal hackers.[5]

24. AAFMAA maintains a separate "Member Privacy Policy" which also includes representations regarding the types of PII AAFMAA collects from its members and the purposes for which it shares that PII.[6]

25. The Member Privacy Policy states that it collects its members' "Social Security Number," "Basic demographic information such as name, address and phone number," "Account balances, account transactions, asset history and credit history," and "Employment History."[7]

26. Through the Member Privacy Policy, AAFMAA also represents that "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[8]

27. The Member Privacy Policy advises AAFMAA members that it shares their PII only in the following scenarios: "For our everyday business purposes," "For our marketing purposes," "For AAFMAA Companies' everyday business purposes," and "For AAFMAA Companies to market to you." Again, these limited scenarios do not include sharing PII with unauthorized third parties, including criminal hackers.[9]

28. AAFMAA maintains a separate "Social Security Number Policy" in which it represents that "[t]he Social Security numbers we collect and maintain are subject to physical, electronic, and procedural safeguards. We take steps to limit access to Social Security numbers and help prevent unauthorized access and disclosure of Social Security numbers."[10]

---

[5] *Id.*
[6] *See* https://www.aafmaa.com/Portals/0/OnlineForms/AAFMAA%20Privacy%20Policy2018.pdf (last visited April 15, 2021).
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *See* https://www.aafmaa.com/about/social-security-number-policy (last visited April 15, 2021).

AAFMAA's Knowledge That It Was and Is a Target of Cyber Threats

29. AAFMAA knew it was a prime target for hackers given the significant amount of sensitive member PII/PHI that it collects and stores.

30. As a financial organization with an acute interest in maintaining the confidentiality of its members' information, AAFMAA is well aware of the numerous data breaches that have occurred throughout the United States and its responsibility for safeguarding users' PII/PHI.

31. Indeed, AAFMAA acknowledged the risk that data breaches can pose to its members in a blog post from September 11, 2017, titled "How Military Families Can Mitigate Risk From Equifax Breach Of Personal Credit Files, By Anthony Powell, Vice President of Operations, AAFMAA Mortgage Services."[11]

32. Other data breaches in the insurance industry, including breaches of the Anthem Healthcare insurance company,[12] the State Farm insurance company,[13] and the Pacific Specialty Insurance Company,[14] also put AAFMAA on notice that it was a prime target for cyber criminals.

33. Indeed, the targeting of insurance companies is common knowledge in the insurance industry. As one industry report prepared by the consulting firm Deloitte noted, "Cyber-attacks in the insurance sector are growing exponentially as insurance companies migrate toward digital channels in an effort to create tighter customer relationships, offer new products and expand their share of customers' financial portfolios."[15]

34. Unfortunately for Mr. Podroykin and other AAFMAA members, AAFMAA did not heed these warnings.

---

[11] *See* https://www.aafmaa.com/learning-hub/blog/post/1861 (last visited April 15, 2021).
[12] *See* https://www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm (last visited April 15, 2021).
[13] *See* https://www.cpomagazine.com/cyber-security/extent-of-damage-for-state-farm-credential-stuffing-attack-still-in-question/ (last visited April 15, 2021).
[14] *See* https://www.prnewswire.com/news-releases/pacific-specialty-insurance-company-provides-notice-of-data-security-incident-301010131.html (last visited April 15, 2021).
[15] *See* https://www2.deloitte.com/be/en/pages/risk/articles/insurance.html (last visited April 15, 2021).

The Data Breach

35. According to the Notice that AAFMAA sent victims of the Data Breach, on January 29, 2021, AAFMAA became aware of suspicious activity on its computer systems and "determined that an unauthorized actor gained access to certain AAFMAA systems between January 2, 2021 and January 31, 2021 and removed and/or viewed certain files from [AAFMAA's] network."[16]

36. In other words, the Notice conceded that PII was targeted and viewed or removed (*i.e.*, stolen) from AAFMAA's systems. AAFMAA disclosed to the Office of the Maine Attorney General that the cause of the Data Breach was an "[e]xternal system breach (hacking)."[17]

37. It was not until on or about March 5, 2021, that AAFMAA sent the Notice to its affected members, including Mr. Podroykin. The Notice informed Mr. Podroykin that his PII had been compromised in the Data Breach; specifically, his name and Social Security number.

38. The Notice of Data Breach did not disclose that additional treasure troves of PII/PHI were stored on AAFMAA's servers, and thus Mr. Podroykin cannot be sure that even more of his PII/PHI was not compromised in the Data Breach. Indeed, AAFMAA disclosed to the Office of the Main Attorney General that the following information was compromised for at least some members in the Data Breach: "Name or other personal identifier in combination with: Financial Account Number or Credit/Debit Card Number (in combination with security code, access code, password or PIN for the account)."

39. At least 161,621 individuals, including Mr. Podroykin, were victims of the AAFMAA Data Breach.[18]

AAFMAA Failed to Comply with Statutory and Regulatory Obligations

40. AAFMA had obligations created by the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, industry standards, state law, and common law to keep Mr. Podroykin's and Class Members' PII/PHI confidential and to protect it from unauthorized access and disclosure.

---

[16] *See* https://media.dojmt.gov/wp-content/uploads/aafSamp.pdf (last visited April 15, 2021).
[17] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/7a48257a-70cf-4399-82ea-c8abf0b5c777.shtml (last visited April 15, 2021).
[18] *Id.*

41. AAFMAA was prohibited by the FTC Act from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

42. Moreover, federal agencies have issued recommendations and guidelines to temper data breaches and the resulting harm to individuals and financial institutions. For example, the 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.[19]

43. 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.[20] Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[21]

44. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor

[19] *Start with Security, A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited April 15, 2021).
[20] *Protecting Personal Information, A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited April 15, 2021).
[21] *Id.*

for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[22]

45. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, 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 FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[23]

46. AAFMAA also failed to comply with commonly accepted industry standards for data security. Security standards commonly accepted among businesses that store PII/PHI 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.

47. AAFMAA is also required by various states' laws and regulations to protect Mr. Podroykin's and Class Members' PII/PHI and to handle any breach of the same in accordance with applicable breach notification statutes.

---

[22] *Start with Security*, *supra* n.19.

[23] *Privacy and Security Enforcement: Press Releases*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited April 9, 2021)

48. In addition to its obligations under federal and state laws, AAFMAA owed a duty to Mr. Podroykin and Class Members whose PII/PHI were entrusted to AAFMAA to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. AAFMAA owed a duty to Mr. Podroykin and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its systems and networks adequately protected the PII/PHI of Mr. Podroykin and Class Members.

49. AAFMAA owed a duty to Mr. Podroykin and Class Members whose PII/PHI were entrusted to AAFMAA to design, maintain, and test its systems to ensure that the PII/PHI in AAFMAA's possession was adequately secured and protected.

50. AAFMAA owed a duty to Mr. Podroykin and Class Members whose PII/PHI was entrusted to AAFMAA to create and implement reasonable data security practices and procedures to protect the PII/PHI in its possession.

51. AAFMAA owed a duty to Mr. Podroykin and Class Members whose PII/PHI was entrusted to AAFMAA to implement processes that would detect a breach on its data security systems in a timely manner.

52. AAFMAA owed a duty to Mr. Podroykin and Class Members whose PII/PHI was entrusted to AAFMAA to act upon data security warnings and alerts in a timely fashion.

53. AAFMAA owed a duty to Mr. Podroykin and Class Members whose PII/PHI was entrusted to AAFMA to disclose if its systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust PII to AAFMAA.

54. AAFMAA owed a duty to Mr. Podroykin and Class Members whose PII/PHI was entrusted to AAFMAA to disclose in a timely and accurate manner when data breaches occurred.

55. AAFMAA owed a duty of care to Mr. Podroykin and Class Members because they were foreseeable and probable victims of any inadequacy in its affirmative development of the systems to maintain PII/PHI and in its affirmative maintenance of those systems.

56. In this case, AAFMAA was fully aware of its obligation to use reasonable measures to protect the PII/PHI of its members, acknowledging as much in its various privacy statements and policies. AAFMAA also knew it was a target for hackers. But despite understanding the consequences of inadequate data security, AAFMAA failed to comply with industry-standard data security requirements.

57. AAFMAA's failure to employ reasonable and appropriate measures to protect against unauthorized access to its members' PII/PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, and various state consumer protection and data breach statutes.

The Value of PII and Effect of the Data Breach

58. It is well known that PII/PHI, including Social Security numbers and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

59. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[24]

60. Consumers place a high value not only on their PII/PHI, 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.

61. 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."[25] 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, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim

[24] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), available at https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin (last visited April 15, 2021).

[25] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), available at https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html (last visited April 15, 2021).

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."[26] And "[f]or some victims of identity theft, a new number actually creates new problems. If the old credit information isn't associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[27]

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

63. PII/PHI is such a valuable commodity to identity thieves that, once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. There is a strong probability that entire batches of stolen information have been dumped on the black market and will be again in the future, meaning Mr. Podroykin and Class Members are at an increased risk of fraud and identity theft for many years to come. Thus, Mr. Podroykin and Class Members must vigilantly monitor their financial and medical accounts for the foreseeable future.

64. There may be a significant time lag between when PII/PHI is stolen and when it is actually misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result,

[26] Social Security Admin., Identity Theft and Your Social Security Number, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited April 9, 2021).
[27] *Id.*

> studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[28]

65. Accordingly, the two years of credit monitoring that AAFMAA offered victims of the Data Breach is woefully inadequate to guard against the risks they face, and in any event does nothing to compensate them for the damages they suffered as a result of the Data Breach.

66. The risk of identity theft is particularly acute where detailed personal information is stolen, such as the PII/PHI that was compromised in the Data Breach.

67. The cyber black-market demonstrates that PII/PHI is a valuable property right.[29] Moreover, its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts, which include heavy prison sentences. This obvious risk/reward analysis illustrates that PII has considerable market value.

68. The value of PII, including PHI, is underscored by the growing number of legitimate marketplaces allowing consumers to monetize their PII.[30]

69. As the result of the Data Breach, Mr. Podroykin and Class Members have suffered or will suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. identity theft and fraud resulting from theft of their PII/PHI;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their online accounts, including financial accounts;

c. losing the inherent value of their PII/PHI;

d. losing the value of AAFMAA's explicit and implicit promises of adequate data security;

---

[28] U.S. Government Accountability Office, *Report to Congressional Requesters* (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited April 15, 2021)

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

[30] *Markets for personal data*, Project VRM, Harvard University, https://cyber.harvard.edu/projectvrm/VRM_Development_Work#Markets_for_personal_data (last visited April 9, 2021).

e. costs associated with purchasing credit monitoring and identity theft protection services;

f. unauthorized access to and misuse of their online accounts;

g. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. costs associated with time spent and the loss of productivity or enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, addressing other varied instances of identity theft – such as credit cards, bank accounts, loans, government benefits, and other services procured using the stolen PII/PHI, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach;

j. the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII/PHI being in the possession of one or more unauthorized third parties; and

k. continued risk of exposure to hackers and thieves of their PII/PHI, which remains in AAFMAA's possession and is subject to further breaches so long as AAFMAA fails to undertake appropriate and adequate measures to protect Mr. Podroykin and Class Members.

70. Additionally, Mr. Podroykin and Class Members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of

consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[31]

71. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[32] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII/PHI to bad actors—would be much higher today.

72. The cost of hosting or processing its members' PII/PHI on or through AAFMAA's databases and systems includes things such as the actual cost of the servers and employee hours needed to process said transactions. One component of the cost of using these services is the explicit and implicit promises AAFMAA made to protect its members' PII/PHI. Because of the value consumers like Mr. Podroykin and the Class Members place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, companies like AAFMAA would have no reason to tout their data security efforts to their actual and potential customers.

73. Had the victims of the Data Breach including Mr. Podroykin and the Class Members known the truth about AAFMAA's data security practices—that AAFMAA would not adequately protect and store their data—they would have either not purchased or would have paid less for goods or services (including life insurance policies) from AAFMAA.

---

[31] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited April 15, 2021).

[32] Hann, Hui, *et al*, The Value of Online Information Privacy: Evidence from the USA and Singapore, at 17, Oct. 2002, *available at* https://www.comp.nus.edu.sg/ ~ipng/research/privacy.pdf

74. Mr. Podroykin and Class Members are at an imminent risk of fraud, criminal misuse of their PII/PHI, and identity theft for years to come as result of the data breach and AAFMAA's deceptive and unconscionable conduct.

CLASS ACTION ALLEGATIONS

75. Pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2), and (b)(3), Mr. Podroykin seeks certification of the following nationwide class:

> **Nationwide Class:** All residents of the United States of America whose PII or PHI was compromised in the Data Breach.

76. The Nationwide Class asserts claims against AAFMAA for negligence (Count I), negligence *per se* (Count II), declaratory judgment (Count III), breach of confidence (Count IV), breach of contract (Count V), unjust enrichment (Count VI), breach of implied contract (Count VII), and violation of Virginia's Consumer Protection Act (Count VIII).

77. Pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2), and (b)(3), Mr. Podroykin seeks certification of Illinois state claims in the alternative to the nationwide claims (with the exception of Count VIII), as well as certification of claims for violations of the Illinois Consumer Fraud Act (Count IX), and the Illinois Uniform Deceptive Trade Practices Act (Count X), on behalf of a subclass of Illinois residents, defined as follows:

> **Illinois Subclass:** All residents of Illinois whose PII or PHI was compromised in the Data Breach.

78. The Nationwide Class and the Illinois Subclass are collectively referred to herein as the "Class."

79. Excluded from the Class are AAFMAA, any entity in which AAFMAA has a controlling interest, and AAFMAA's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, members of their judicial staff, and any judge sitting in the presiding court system who may hear an appeal of any judgment entered.

80. **Risk of Inconsistent or Varying Adjudications. Fed. R. Civ. P. 23(b)(1).** As the proposed Class include tens of thousands of members, there is significant risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for AAFMAA. For example, injunctive relief may be entered in multiple cases, but the ordered relief may vary, causing AAFMAA to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which it will comply. Class action status is also warranted because prosecution of separate actions by the members of the Class would create a risk of adjudications with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

81. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. AAFMAA has admitted that at least 161,621 individuals were victims of the AAFMAA Data Breach.

82. **Commonality and Predominance. Fed. R. Civ. P. 23(a)(2) and (b)(3).** This action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include, but are not limited to:

a. Whether AAFMAA knew or should have known that its computer and data storage systems were vulnerable to attack;

b. Whether AAFMAA omitted or misrepresented material facts regarding the security of its computer and data storage systems and their inability to protect vast amounts of sensitive data, including Mr. Podroykin and Class Members' PII/PHI;

c. Whether AAFMAA failed to take adequate and reasonable measures to ensure such computer and data systems were protected;

d. Whether AAFMAA owed a duty of care to Mr. Podroykin and Class Members, as alleged above;

e. Whether AAFMAA breached the duties of care it owed to Mr. Podroykin and Class Members;

f. Whether AAFMAA failed to take available steps to prevent and stop the Data Breach from happening;

g. Whether AAFMAA failed to disclose the material facts that it did not have adequate computer systems and security practices to safeguard PII/PHI;

h. Whether AAFMAA's failure to secure Mr. Podroykin's and Class Members' PII/PHI in the manner alleged violated federal, state, and local laws and regulations, or industry standards;

i. Whether AAFMAA was negligent, reckless, or intentionally indifferent in its representations or omissions to Mr. Podroykin and Class Members concerning its security protocols;

j. Whether AAFMAA was negligent in making misrepresentations or omissions to Mr. Podroykin and Class Members;

k. Whether AAFMAA was negligent in establishing, implementing, and following security protocols;

l. Whether Mr. Podroykin's and Class Members' PII/PHI was compromised and exposed as a result of the Data Breach and the extent of that compromise and exposure;

m. Whether AAFMAA's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unauthorized access to, compromise, and/or theft of Mr. Podroykin's and Class Members' PII/PHI;

n. Whether AAFMAA's conduct amounted to violations of state statutes, as alleged below;

o. Whether, as a result of AAFMAA's conduct, Mr. Podroykin and Class Members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled;

p. Whether, as a result of AAFMAA's conduct, Mr. Podroykin and Class Members are entitled to injunctive, equitable, declaratory and/or other relief and, if so, the nature of such relief;

q. Whether Mr. Podroykin and Class Members are entitled to compensatory damages;

r. Whether Mr. Podroykin and Class Members are entitled to punitive damages; and

s. Whether Mr. Podroykin and Class Members are entitled to statutory damages.

83. **Typicality. Fed. R. Civ. P. 23(a)(3).** Mr. Podroykin's claims are typical of other Class Members' claims because Mr. Podroykin and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way.

84. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Mr. Podroykin is an adequate representative of the Class. Mr. Podroykin is a member of the Class. Mr. Podroykin has no conflicts of interest with the Class. Mr. Podroykin has retained counsel competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation and consumer protection claims. Mr. Podroykin intends to vigorously prosecute this case and will fairly and adequately protect the interests of the Class.

85. **Injunctive and Declaratory Relief. Fed. R. Civ. P. 23(b)(2).** Class certification is also appropriate under Rule 23(b)(2). AAFMAA, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole. Moreover, AAFMAA continues to maintain its inadequate security practices, retains possession of Mr. Podroykin's and Class Members' PII/PHI, and has not been forced to change its practices or to relinquish PII/PHI by nature of other civil suits or government enforcement actions, thus making injunctive and declaratory relief a live issue and appropriate to the Class as a whole.

86. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to

individual plaintiffs and Class Members may not be sufficient to justify individual litigation. Here, the damages suffered by Mr. Podroykin and the Class Members are relatively small compared to the burden and expense required to individually litigate their claims against AAFMAA, a sophisticated financial institution, and thus, individual litigation to redress AAFMAA's wrongful conduct would be impracticable. Individual litigation by each class member would also strain the court system. Moreover, individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contract, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

(On behalf of Plaintiff and the Nationwide Class or, in the alternative, on behalf of Plaintiff and the Illinois Subclass)

87. Mr. Podroykin repeats the allegations in paragraphs 1 – 86 of this Complaint, as if fully alleged herein.

88. AAFMAA owed a duty of care to Mr. Podroykin and Class Members to use reasonable means to secure and safeguard the entrusted PII/PHI, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems, as alleged herein. These common law duties existed because Mr. Podroykin and Class Members were the foreseeable and probable victims of any inadequate security practices in AAFMAA's affirmative development and maintenance of its data security systems. In fact, not only was it foreseeable that Mr. Podroykin and Class Members would be harmed by the failure to protect their PII/PHI because hackers routinely attempt to steal such information and use it for nefarious purposes, AAFMAA knew that it was more likely than not Mr. Podroykin and other Class Members would be harmed by such exposure and theft of their PII/PHI.

89. AAFMAA's duties to use reasonable security measures also arose as a result of the special relationship that existed between AAFMAA, on the one hand, and Mr. Podroykin and Class Members, on the other hand. This special relationship arose because Mr. Podroykin and Class Members entrusted AAFMAA with their PII/PHI as part of the process for applying for life insurance and other financial services products. AAFMAA alone could have ensured that its data security systems and practices were sufficient to prevent or minimize the Data Breach.

90. AAFMAA's duties to use reasonable data security measures also arose under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII/PHI. Various FTC publications and data security breach orders further form the basis of AAFMAA's duties. In addition, individual states have enacted statutes based on the FTC Act, such as the Virginia Consumer Protection Act and the Illinois Uniform Deceptive Trade Practices Act, that also created a duty.

91. AAFMAA breached the aforementioned duties when it failed to use security practices that would protect the PII provided to it by Mr. Podroykin and Class Members, thus resulting in unauthorized exposure and third party access to Mr. Podroykin's and Class Members' PII/PHI.

92. AAFMAA further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Mr. Podroykin's and Class Members' PII/PHI within its possession, custody, and control.

93. As a direct and proximate cause of AAFMAA's failure to adequately develop and maintain its data security systems, and its failure to use appropriate security practices, Mr. Podroykin and Class Members' PII/PHI was exposed, disseminated, and made available to unauthorized third parties.

94. AAFMAA admitted that Mr. Podroykin's and Class Members' PII was wrongfully disclosed and/or stolen as a result of the Data Breach. Given the scope of the Breach, it is likely that

Mr. Podroykin's and Class Members' PHI was also wrongfully disclosed and/or stolen as a result of the Data Breach.

95. The Data Breach caused direct and substantial damages to Mr. Podroykin and Class Members, as well as the likelihood of future and imminent harm through the dissemination of their PII/PHI and the greatly enhanced risk of credit fraud and identity theft.

96. By engaging in the foregoing acts and omissions, AAFMAA committed the common law tort of negligence. For all the reasons stated above, AAFMAA's conduct was negligent and departed from reasonable standards of care including by, but not limited to: failing to adequately limit access to and protect the PII/PHI; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Mr. Podroykin's and Class Members' PII/PHI.

97. But for AAFMAA's wrongful and negligent breach of its duties owed to Mr. Podroykin and Class Members, their PII/PHI would not have been compromised.

98. Neither Mr. Podroykin nor Class Members contributed to the Data Breach or subsequent misuse of their PII/PHI as described in this Complaint.

99. As a direct and proximate result of AAFMAA's negligence, Mr. Podroykin and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by AAFMAA, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT II

***NEGLIGENCE* PER SE**

(On behalf of Plaintiff and the Nationwide Class or, in the alternative, on behalf of Plaintiff and the Illinois Subclass)

100. Mr. Podroykin repeats the allegations in paragraphs 1 – 86 of this Complaint, as if fully alleged herein.

101. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by AAFMAA of failing to use reasonable measures to protect PII/PHI. Various FTC publications and orders also form the basis of AAFMAA's duty.

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

103. AAFMAA's violation of Section 5 of the FTC Act (and similar state statutes, such as the Virginia Consumer Protection Act and the Illinois Uniform Deceptive Trade Practices Act) constitutes negligence *per se*.

104. Mr. Podroykin and Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

105. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of defendants' failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Mr. Podroykin and Class Members.

106. As a direct and proximate result of AAFMAA's negligence, Mr. Podroykin and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of

identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by AAFMAA, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT III

DECLARATORY JUDGMENT

(On behalf of Plaintiff and the Nationwide Class or, in the alternative, on behalf of Plaintiff and the Illinois Subclass)

107. Mr. Podroykin repeats the allegations in paragraphs 1 – 86 of this Complaint, as if fully alleged herein.

108. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

109. An actual controversy has arisen in the wake of the Data Breach regarding AAFMAA's present and prospective common law and other duties to reasonably safeguard its users' PII/PHI, and whether AAFMAA is currently maintaining data security measures adequate to protect Mr. Podroykin's and Class Members from further data breaches that compromise their PII/PHI. Mr. Podroykin and Class Members remain at imminent risk that further compromises of their PII/PHI will occur in the future. This is true even if they are not actively using AAFMAA's products or services.

110. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. AAFMAA continues to owe a legal duty to secure users' PII/PHI and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

b. AAFMAA continues to breach this legal duty by failing to employ reasonable measures to secure Mr. Podroykin's and Class Members' PII/PHI.

111. The Court also should issue corresponding prospective injunctive relief pursuant to 28 U.S.C. § 2202, requiring AAFMAA to employ adequate security practices consistent with law and industry standards to protect its users' PII/PHI.

112. If an injunction is not issued, Mr. Podroykin and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of AAFMAA. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Mr. Podroykin and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

113. The hardship to Mr. Podroykin and Class Members if an injunction does not issue exceeds the hardship to AAFMAA if an injunction is issued. Among other things, if another data breach occurs at AAFMAA, Mr. Podroykin and Class Members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to AAFMAA of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and AAFMAA has a pre-existing legal obligation to employ such measures.

114. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at AAFMAA, thus eliminating additional injuries that would result to Plaintiffs, Class Members, and the tens of thousands of other AAFMAA members and their families whose PII/PHI would be further compromised.

COUNT IV

BREACH OF CONFIDENCE

(On behalf of Plaintiff and the Nationwide Class or, in the alternative, on behalf of Plaintiff and the Illinois Subclass)

115. Mr. Podroykin repeats the allegations in paragraphs 1 – 86 of this Complaint, as if fully alleged herein.

116. At all times during Mr. Podroykin's and Class Members' interactions with AAFMAA, AAFMAA was fully aware of the confidential and sensitive nature of Mr. Podroykin's and Class Members' PII/PHI.

117. As alleged herein and above, AAFMAA's relationship with Mr. Podroykin and Class Members was governed by terms and expectations that Mr. Podroykin's and Class Members' PII/PHI would be collected, stored, and protected in confidence, and would not be disclosed to the public or any unauthorized third parties.

118. Mr. Podroykin and Class Members provided their respective PII/PHI to AAFMAA with the explicit and implicit understandings that AAFMAA would protect and not permit their PII/PHI to be disseminated to the public or any unauthorized parties.

119. Mr. Podroykin and Class Members also provided their respective PII/PHI to AAFMAA with the explicit and implicit understandings that AAFMAA would take precautions to protect the PII/PHI from unauthorized disclosure, such as following basic principles of encryption and information security practices.

120. AAFMAA voluntarily received in confidence Mr. Podroykin's and Class Members' PII/PHI with the understanding that PII/PHI would not be disclosed or disseminated to the public or any unauthorized third parties.

121. Due to AAFMAA's failure to prevent, detect, and avoid the Data Breach from occurring by following best information security practices to secure Mr. Podroykin's and Class Members' PII/PHI, Mr. Podroykin's and Class Members' PII/PHI was disclosed and

misappropriated to the public and unauthorized third parties beyond Mr. Podroykin's and Class Members' confidence, and without their express permission.

122. But for AAFMAA's disclosure of Mr. Podroykin's and Class Members' PII/PHI in violation of the parties' understanding of confidence, their PII/PHI would not have been compromised, stolen, viewed, accessed, and/or used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Mr. Podroykin's and Class Members' PII/PHI, as well as the resulting damages.

123. The injury and harm Mr. Podroykin and Class Members suffered was the reasonably foreseeable result of AAFMAA's unauthorized disclosure of Mr. Podroykin's and Class Members' PII/PHI. AAFMAA knew its computer systems and technologies for accepting, securing, and storing Mr. Podroykin's and Class Members' PII/PHI had serious security vulnerabilities because AAFMAA failed to observe even basic information security practices or correct known security vulnerabilities.

124. As a direct and proximate result of AAFMAA's breaches of confidence, Mr. Podroykin and Class Members have been injured and were damaged as discussed herein and as will be proven at trial.

125. As a direct and proximate result of AAFMAA's breach of confidence, Mr. Podroykin and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by AAFMAA, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT V

BREACH OF CONTRACT

(On behalf of Plaintiff and the Nationwide Class or, in the alternative, on behalf of Plaintiff and the Illinois Subclass)

126. Mr. Podroykin repeats the allegations in paragraphs 1 – 86 of this Complaint, as if fully alleged herein and asserts this claim in the alternative to the Breach of Implied Contract claim (Count VI) and Unjust Enrichment claim (Count VII), to the extent necessary.

127. AAFMAA's Member Privacy Policy is an agreement between AAFMAA and its members. Any non-AAFMAA members who are members of the Class (*e.g.*, family members of AAFMAA members, who are not AAFMAA members themselves, but whose PII/PHI was provided to AAFMAA for the purpose of applying for life insurance other financial services) are the clear intended third-party beneficiaries of the Member Privacy Policy.

128. The Member Privacy Policy states that AAFMAA collects its members' "Social Security Number," "Basic demographic information such as name, address and phone number," "Account balances, account transactions, asset history and credit history," and "Employment History."[33] AAFMAA also collects PHI from its members, as alleged above.

129. Through the Member Privacy Policy, AAFMAA also represents that "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[34]

130. The Member Privacy Policy advises AAFMAA members that it shares their PII only in the following scenarios: "For our everyday business purposes," "For our marketing purposes," "For AAFMAA Companies' everyday business purposes," and "For AAFMAA Companies to market to you." These limited scenarios do not include sharing PII/PHI with unauthorized third parties.[35]

131. AAFMAA, on the one hand, and Mr. Podroykin and Class Members on the other hand, formed a contract pursuant to the Member Privacy Policy when Mr. Podroykin and Class

[33] *Id.*
[34] *Id.*
[35] *Id.*

Members provided PII/PHI to AAFMAA for the purposes of obtaining life insurance policies and other financial services from AAFMAA.

132. AAFMAA breached the Member Privacy Policy contract, to the detriment of Mr. Podroykin and Class Members, by failing to protect their PII/PHI. Specifically, AAFMAA (1) failed to use reasonable measures or "security measures that comply with federal law" to protect Mr. Podroykin and Class Members' PII/PHI; and (2) disclosed that PII/PHI to unauthorized third parties, in violation of the agreement.

133. Additionally, the various life insurance policies and other financial services contracts between Mr. Podroykin and Class Members, on the one hand, and AAFMAA on the other hand, contemplated payments by Mr. Podroykin and Class Members that were intended to cover, in part, use of reasonable security measures to protect Mr. Podroykin's and Class Members' PII/PHI.

134. AAFMAA breached these additional contracts, to the detriment of Mr. Podroykin and Class Members, by failing to protect their PII/PHI. Specifically, AAFMAA (1) failed to use reasonable measures to protect Mr. Podroykin and Class Members' PII/PHI; and (2) disclosed that PII/PHI to unauthorized third parties, in violation of these additional contracts.

135. As a direct result of AAFMAA's breach of contract, Mr. Podroykin and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by AAFMAA, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

136. Additionally, because Mr. Podroykin and Class Members continue to be parties to the Member Privacy Policy contract with AAFMAA, and because damages may not provide a complete remedy for the breaches alleged herein, Mr. Podroykin and Class Members are therefore entitled to specific performance of the contract to ensure data security measures necessary to properly effectuate the contracts and maintain the security of their PII/PHI from unlawful exposure and/or theft.

137. AAFMAA's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract, and AAFMAA is liable to Mr. Podroykin and Class Members for associated damages and specific performance.

COUNT VI

BREACH OF IMPLIED CONTRACT

(On behalf of Plaintiff and the Nationwide Class or, in the alternative, on behalf of Plaintiff and the Illinois Subclass)

138. Mr. Podroykin repeats the allegations in paragraphs 1 – 86 of this Complaint, as if fully alleged herein and asserts this claim in the alternative to the Breach of Contract claim (Count V) and Unjust Enrichment claim (Count VII), to the extent necessary.

139. AAFMAA invited applicants, including Mr. Podroykin and Class Members, to provide their PII/PHI in order to obtain life insurance and other financial services products. As consideration for the life insurance and other financial services products AAFMAA was to administer, Mr. Podroykin and Class Members provided their PII/PHI and other valuable consideration to AAFMAA. When Mr. Podroykin and Class Members provided their PII/PHI to AAFMAA, they entered into implied contracts by which AAFMAA agreed to protect their PII/PHI and only use it solely to provide the bargained-for services. As part of the offer, AAFMAA would safeguard the PII/PHI using reasonable or industry-standard means.

140. Accordingly, Mr. Podroykin and Class Members accepted AAFMAA's offer to provide life insurance and other financial services and provided AAFMAA their PII/PHI and other valuable consideration in exchange.

141. Mr. Podroykin and Class Members fully performed their obligations under the implied contracts with AAFMAA. However, AAFMAA breached the implied contracts by failing to safeguard Mr. Podroykin's and Class Members' PII/PHI.

142. As a direct result of AAFMAA's breach of implied contract, Mr. Podroykin and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by AAFMAA, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

143. Additionally, because Mr. Podroykin and Class Members continue to be parties to the implied contract with AAFMAA, and because damages may not provide a complete remedy for the breaches alleged herein, Mr. Podroykin and Class Members are therefore entitled to specific performance of the contracts to ensure data security measures necessary to properly effectuate the contracts and maintain the security of their PII/PHI from unlawful exposure and/or theft.

144. AAFMAA's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract, and AAFMAA is liable to Mr. Podroykin and Class Members for associated damages and specific performance.

COUNT VII

UNJUST ENRICHMENT

(On behalf of Plaintiff and the Nationwide Class or, in the alternative, on behalf of Plaintiff and the Illinois Subclass)

145. Mr. Podroykin repeats the allegations in paragraphs 1 – 86 of this Complaint, as if fully alleged herein and asserts this claim in the alternative to the Breach of Contract claim (Count V) and Breach of Implied Contract claim (Count VI), to the extent necessary.

146. Mr. Podroykin and Class Members have an interest, both equitable and legal, in their PII/PHI that was conferred upon, collected by, and maintained by AAFMAA and that was ultimately compromised and/or stolen in the Data Breach.

147. Additionally, Mr. Podroykin and Class Members paid premiums for life insurance policies and/or fees for other financial services which were intended, in part, to be used to pay for the necessary data security measures to protect their PII/PHI. Had Mr. Podroykin and Class Members known that AAFMAA would not adequately safeguard their PII/PHI, they would have paid less for or would not have purchased life insurance or other financial services from AAFMAA.

148. AAFMAA, by way of its acts and omissions, knowingly and deliberately enriched itself by saving the costs it reasonably should have expended on security measures to secure Mr. Podroykin's and Class Members' PII/PHI.

149. AAFMAA also understood and appreciated that the PII/PHI pertaining to Mr. Podroykin and Class Members was private and confidential and its value depended on AAFMAA maintaining the privacy and confidentiality of that PII/PHI.

150. Instead of providing for a reasonable level of security that would have prevented the Data Breach—as is common practice among companies entrusted with such PII—AAFMAA instead consciously and opportunistically calculated to increase its own revenues at the expense of Mr. Podroykin and Class Members. AAFMAA continued to obtain the benefits conferred on it by Mr. Podroykin and Class Members. The benefits conferred upon, received, and enjoyed by AAFMAA

were not conferred officiously or gratuitously, and it would be inequitable and unjust for AAFMAA to retain these benefits.

151. Mr. Podroykin and Class Members, on the other hand, suffered as a direct and proximate result. As a direct result of AAFMAA's unjust enrichment, Mr. Podroykin and Class Members have been injured. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by AAFMAA, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

152. Thus, AAFMAA engaged in opportunistic conduct in spite of its duties to Mr. Podroykin and Class Members, wherein it profited from interference with Mr. Podroykin's and Class Members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit AAFMAA to retain the benefits it derived as a consequence of its conduct.

153. Accordingly, Mr. Podroykin, on behalf of himself and the Class, respectfully requests that this Court award relief in the form of restitution or disgorgement in the amount of the benefit conferred on AAFMAA as a result of its wrongful conduct, including specifically, the amounts that AAFMAA should have spent to provide reasonable and adequate data security to protect Mr. Podroykin's and Class Members' PII/PHI and/or compensatory damages.

COUNT VIII

VIRGINIA'S CONSUMER PROTECTION ACT

Va. Code Ann. §§ 59.1-196, *et seq.*

(On behalf of Plaintiff and the Nationwide Class or, in the alternative, on behalf of Plaintiff and the Illinois Subclass)

154. Mr. Podroykin repeats the allegations in paragraphs 1 – 86 of this Complaint, as if fully alleged herein.

155. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

156. AAFMAA is a "person" as defined by Va. Code Ann. § 59.1-198.

157. AAFMAA is a "supplier," as defined by Va. Code Ann. § 59.1-198.

158. AAFMAA engaged in the complained-of conduct in connection with "consumer" transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198. AAFMAA advertised, offered, or sold goods or services used primarily for personal, family or household purposes.

159. AAFMAA engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Mr. Podroykin and Class Members' PII/PHI, which was a direct and proximate cause of the Data Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Mr. Podroykin's and Class Members' PII/PHI, including duties

imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Mr. Podroykin's and Class Members' PII/PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Mr. Podroykin and Class Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Mr. Podroykin's and Class Members' PII/PHI; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Mr. Podroykin and Class Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45.

160. AAFMAA intended to mislead Mr. Podroykin and Class Members and induce them to rely on its misrepresentations and omissions.

161. AAFMAA's representations and omissions were material because they were likely to deceive reasonable consumers, including Mr. Podroykin and Class Members, about the adequacy of AAFMAA's computer and data security and the quality of the AAFMAA brand.

162. Had AAFMAA disclosed to Mr. Podroykin and Class Members that its data systems were not secure and, thus, vulnerable to attack, AAFMAA would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, AAFMAA received, maintained, and compiled Mr. Podroykin's and Class Members' PII/PHI as part of the services AAFMAA provided and for which Mr. Podroykin and Class Members' paid without advising Mr. Podroykin and Class Members that AAFMAA's data security practices were insufficient to maintain the safety and confidentiality of Mr. Podroykin's and Class Members'

PII/PHI. Accordingly, Mr. Podroykin and Class Members acted reasonably in relying on AAFMAA's misrepresentations and omissions, the truth of which they could not have discovered.

163. AAFMAA had a duty to disclose these facts due to the circumstances of this case and the sensitivity and extensivity of the PII/PHI in its possession. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Mr. Podroykin and Class Members—and AAFMAA, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in AAFMAA. AAFMAA's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, while purposefully withholding material facts from Mr. Podroykin and Class Members that contradicted these representations.

164. The above-described deceptive acts and practices also violated the following provisions of VA Code § 59.1-200(A):

a. Misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits;

b. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and

c. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised.

165. AAFMAA acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Mr. Podroykin's and Class Members' rights. Past breaches in the insurance and financial services industries put it on notice that its security and privacy protections were inadequate. An award of punitive damages would serve to punish AAFMAA for its wrongdoing, and warn or deter others from engaging in similar conduct.

166. As a direct result of AAFMAA's deceptive acts or practices, Mr. Podroykin and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by AAFMAA, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

167. AAFMAA's violations present a continuing risk to Mr. Podroykin and Class Members as well as to the general public.

168. Mr. Podroykin and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of $1,000 per violation if the conduct is found to be willful or, in the alternative, $500 per violation; restitution, injunctive relief; punitive damages; and attorneys' fees and costs.

/

/

/

/

/

COUNT IX

ILLINOIS CONSUMER FRAUD ACT

815 Ill. Comp. Stat. §§ 505, *et seq.*

(On behalf of Plaintiff and the Illinois Subclass)

169. Mr. Podroykin repeats the allegations in paragraphs 1 – 86 of this Complaint, as if fully alleged herein.

170. AAFMAA is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

171. Mr. Podroykin and Illinois Subclass Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

172. AAFMAA's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

173. AAFMAA's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Mr. Podroykin's and Illinois Subclass Members' PII/PHI, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the insurance and financial services industries, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Mr. Podroykin's and Illinois Subclass Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Mr. Podroykin's and Illinois Subclass Members' PII/PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Mr. Podroykin's and Illinois Subclass Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Mr. Podroykin's and Illinois Subclass Members' PII/PHI; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Mr. Podroykin's and Illinois Subclass Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

174. AAFMAA's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AAFMAA's data security and ability to protect the confidentiality of consumers' PII/PHI.

175. AAFMAA intended to mislead Mr. Podroykin and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

176. The above unfair and deceptive practices and acts by AAFMAA were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

177. AAFMAA acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Mr. Podroykin's and Illinois Subclass Members'

rights. AAFMAA's knowledge of past breaches in the insurance industry put it on notice that its security and privacy protections were inadequate.

178. As a direct and proximate result of AAFMAA's unfair, unlawful, and deceptive acts and practices, Mr. Podroykin and Subclass Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by AAFMAA, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

179. Mr. Podroykin and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT IX

ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT

815 Ill. Comp. Stat. §§ 510/2, *et seq.*

(On behalf of Plaintiff and the Illinois Subclass)

180. Mr. Podroykin repeats the allegations in paragraphs 1 – 86 of this Complaint, as if fully alleged herein.

181. AAFMAA is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

182. AAFMAA engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

183. AAFMAA's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Mr. Podroykin's and Illinois Subclass Members' PII/PHI, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the insurance and financial services industries, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Mr. Podroykin's and Illinois Subclass Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Mr. Podroykin's and Illinois Subclass Members' PII/PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Mr. Podroykin's and Illinois Subclass Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, and

the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Mr. Podroykin's and Illinois Subclass Members' PII/PHI; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Mr. Podroykin's and Illinois Subclass Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

184. AAFMAA's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AAFMAA's data security and ability to protect the confidentiality of consumers' PII/PHI.

185. The above unfair and deceptive practices and acts by AAFMAA were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Mr. Podroykin and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

186. As a direct and proximate result of AAFMAA's unfair, unlawful, and deceptive trade practices, Mr. Podroykin and Subclass Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by AAFMAA, reviewing bank statements, payment card statements, and credit reports; expenses and time spent

initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

187. Mr. Podroykin and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorneys' fees.

REQUEST FOR RELIEF

WHEREFORE, Mr. Podroykin, individually and on behalf of all Class Members proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against AAFMAA as follows:

1) For an Order certifying the Nationwide Class and the Illinois Subclass, as defined herein, and appointing Mr. Podroykin and Mr. Podroykin's counsel to represent the Class as alleged herein;
2) For injunctive and other equitable relief as is necessary to protect the interests of Mr. Podroykin and Class Members;
3) For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;
4) For an award of statutory damages and punitive damages, as allowed by law in an amount to be determined;
5) For an award of restitution or disgorgement, in an amount to be determined;
6) For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
7) For prejudgment interest on all amounts awarded; and
8) Such other and further relief as the Court may deem just and proper.

JURY DEMAND

Mr. Podroykin, on behalf of himself and the Class of all others similarly situated, hereby demands a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Respectfully Submitted,
TYCKO & ZAVAREEI LLP

Dated: May 10, 2021

/s/ Glenn E. Chappel
Glenn E. Chappell (Bar No. 92153)
gchappell@tzlegal.com
Hassan A. Zavareei*
hzavareei@tzlegal.com
Mark A. Clifford*
mclifford@tzlegal.com
1828 L Street NW, Suite 1000
Washington, D.C. 20036
Tel.: (202) 973-0900
Fax: (202) 973-0950

Melissa S. Weiner*
mweiner@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
800 LaSalle Avenue, Suite 2150
Minneapolis, MN 55402
Tel.: (612) 389-0600
Fax: (612) 389-0610,

Jason H. Alperstein*
alperstein@kolawyers.com
Kristen L. Cardoso*
cardoso@kolawyers.com
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
1 West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel.: (954) 525-4100
Fax: (954) 525-4300

Counsel for Plaintiff Podroykin and the Proposed Classes

**pro hac vice* application forthcoming

ClassAction.org