THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

A.A., a minor, by and through his natural parent, STEVE ALTES, PAUL BRIGHT and BILLY CHOI, on behalf of themselves and all others similarly situated, Plaintiffs, vs. AFTRA RETIREMENT FUND, Defendant.	Case No.: _____ **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs A.A. (a minor, by and through his natural parent, Steve Altes), Paul Bright and Billy Choi ("Plaintiffs") bring this Class Action Complaint against AFTRA Retirement Fund ("AFTRA" or "Defendant"), as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against AFTRA to seek damages for Plaintiffs and the class of consumers who they seek to represent, as well as other equitable relief, including without limitation injunctive relief designed to protect the very sensitive information of Plaintiffs and other consumers. This action arises from AFTRA's failure to properly secure and safeguard personal identifiable information, including without limitation, names, Social Security numbers, addresses and dates of birth (collectively, "personal identifiable information" or "PII"). Plaintiffs also allege AFTRA failed to provide timely, accurate, and adequate notice to Plaintiffs and similarly situated AFTRA current and former fund participants ("Class Members") that their PII had been lost and precisely what types of information was unencrypted and in the possession of unknown third parties.

2. The AFTRA Retirement Fund has provided retirement benefits to performers – including actors, broadcasters and voice professionals – for over 50 years. The fund was established as a result of collective bargaining between the American Federation of Television and

Radio Artists and contributing entertainment employers. The AFTRA Retirement Fund claims to be a separate legal entity from the well-known union, the Screen Actors Guild, also known as SAG-AFTRA. In 2017, the AFTRA Health Fund merged with the SAG-Producers Health Plan to form the SAG-AFTRA Health Plan ("Health Plan"). Following that merger, the AFTRA Retirement Fund supported the Health Plan as a business associate.

3. On or about February 25, 2020, AFTRA notified state Attorneys General and many of its fund participants about a widespread data breach involving sensitive PII of certain current and former plan members of the SAG-AFTRA Health Plan. AFTRA explained that, on or about October 28, 2019, AFTRA received an alert of suspicious activity in its network and quickly discovered that certain files and folders on its network had been breached by unauthorized hackers between October 24, 2019 and October 28, 2019. AFTRA then determined that the exfiltrated PII included AFTRA Health Plan's participants' name, address, Social Security number, AFTRA Number, date of birth, date of death, and "Past Information about: eligibility, dependent(s), claims, earnings, contributions, and beneficiaries."

4. On or about December 17, 2020, AFTRA began notifying certain fund participants in the AFTRA Retirement Fund about the October 2019 breach – more than a year after discovering the breach and conducting an investigation, and nearly 10 months after notifying state Attorneys General. In this December 2020 *Notice of Data Breach*, AFTRA claimed that participants in the AFTRA Retirement Fund (not the Health Plan) were affected by this expansive breach, and the exposed sensitive PII in this instance was limited to name, Social Security number, addresses and date of birth (the "Data Breach").

5. Plaintiffs in this action were all participants of the AFTRA Retirement Fund, not the Health Plan, and were not notified about the Data Breach until on or about December 17, 2020.

6. This PII was compromised due to AFTRA's negligent and/or careless acts and omissions and the failure to protect consumers' data. In addition to AFTRA's failure to prevent the Data Breach, AFTRA failed to provide timely notice to the affected participants: it took AFTRA four months to provide notice to the Health Plan members and over a year to notify the

AFTRA Retirement Fund members. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk to identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes. Hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members.

7. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of AFTRA's failure to: (i) adequately protect consumers' PII; (ii) warn consumers of its inadequate information security practices; and (iii) effectively monitor AFTRA's network for security vulnerabilities and incidents. AFTRA's conduct amounts to negligence and violates federal and state statutes.

8. Plaintiffs and Class Members have suffered injury as a result of AFTRA's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) deprivation of rights they possess under the California Unfair Competition Law, (Cal. Business & Professions Code § 17200, *et seq*.) and similar consumer protection statutes in other states; and (v) the continued and certainly an increased risk to their PII, which remains in AFTRA's possession and is subject to further unauthorized disclosures so long as AFTRA fails to undertake appropriate and adequate measures to protect the PII. This risk will remain for the lifetimes of Plaintiffs and Class Members.

9. AFTRA disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or at the very least negligently failing to take and implement adequate and reasonable measures to ensure that its retirement fund members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a

continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

10. Plaintiff A.A. is a Citizen of California residing in Los Angeles County, California. Steve Altes is A.A.'s father and legal guardian. A.A. is not a member of the SAG-AFTRA union. On or about August 22, 2014, A.A. received a waiver to appear in a union television commercial. A.A. received AFTRA's *Notice of Data Breach*, dated December 17, 2020, on or about that date. The *Notice* was addressed to "Parent of Guardian of [A.A.]" If Mr. Altes had known that AFTRA would not adequately protect A.A.'s PII, he would not have allowed AFTRA access to this sensitive and private information.

11. Plaintiff Paul Bright is a Citizen of Oregon residing in Clackamas County, Oregon. Mr. Bright was a union member until in or about 2006, at which time he elected financial core status. This made him ineligible to draw retirement funds. Mr. Bright received AFTRA's *Notice of Data Breach*, dated December 17, 2020, on or about that date. If Mr. Bright had known that AFTRA would not adequately protect his PII, he would not have allowed AFTRA access to this sensitive and private information.

12. Plaintiff Billy Choi is a Citizen of California residing in Ventura County, California. Mr. Choi has been a union member since in or about 2013. Mr. Choi received AFTRA's *Notice of Data Breach*, dated December 17, 2020, on or about that date. If Mr. Choi had known that AFTRA would not adequately protect his PII, he would not have allowed AFTRA access to this sensitive and private information.

13. Defendant AFTRA Retirement Fund is a retirement fund with its principal place of business at 261 Madison Avenue, 7th floor, New York, NY 10016. AFTRA claims to have provided retirement benefits to performers for over 50 years. According to AFTRA, the "AFTRA Retirement Fund is a separate legal entity from SAG-AFTRA, the union. The AFTRA Retirement Fund is not a subsidiary, department or agent of SAG-AFTRA. No portion of SAG-AFTRA's union dues goes to support the AFTRA Retirement Fund's benefits or operational expenses, except

for the contributions that SAG-AFTRA makes to provide retirement benefits for its own employees."[1]

14. Moreover, "there are statutory restrictions regarding the sharing of information between the [union and the AFTRA Retirement Fund]," and "[t]he AFTRA Retirement Fund is a jointly administered fund governed by a Board of Trustees with equal representation from both SAG-AFTRA and contributing industry employers."[2]

15. 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 Plaintiffs. Plaintiffs 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.

16. All of Plaintiffs' claims stated herein are asserted against AFTRA and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

17. 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 Plaintiffs A.A. and Mr. Choi are Citizens of California; Plaintiff Bright, a citizen of Oregon) is a citizen of a state different from Defendant to establish minimal diversity..

18. The Southern District of New York has personal jurisdiction over Defendant named in this action because Defendant is headquartered in this District and conducts substantial business in New York and this District through its headquarters, offices, and affiliates.

---

[1] AFTRA *About Us* webpage, *available at*: https://aftraretirement.org/Home/learn_about_us/about_us.aspx.

[2] AFTRA *Registering with the AFTRA Retirement Fund, available at*: https://aftraretirement.org/docs/default-source/default-document-library/registering-with-the-aftra-retirement-fund-your-first-step-toward-benefits4c0d15b1d2446ae9a23dff00001d7895.pdf?sfvrsn=0

19. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered in this District and has caused harm to Plaintiffs and Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

Background

20. AFTRA promises that it will protect its members' privacy and remain in compliance with statutory privacy requirements. For example, AFTRA states on its website that "[t]he AFTRA Retirement Fund respects your privacy and is committed to safeguarding your personal information."[3] AFTRA also states: "We take appropriate physical, electronic, and other security measures to help safeguard personal information from unauthorized access, alteration, or disclosure."[4]

21. Plaintiffs and the Class Members, as current and former participants in the AFTRA Retirement Fund, relied on this sophisticated entity 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. Consumers, in general, demand security to safeguard their PII, especially when Social Security numbers and other sensitive PII is involved.

22. AFTRA had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

23. Beginning on or about February 25, 2020, AFTRA notified many of its fund participants and state Attorneys General about a widespread data breach involving sensitive PII of certain current and former plan members of the SAG-AFTRA Health Plan. AFTRA explained that, on or about October 28, 2019, AFTRA received an alert of suspicious activity in its network and quickly discovered that certain files and folders on its network had been breached by unauthorized

[3] AFTRA *Website Privacy Policy, available at*: https://www.aftraretirement.org/Home/legal/web_privacy_policy.aspx
[4] *Id.*

hackers between October 24, 2019 and October 28, 2019. AFTRA then determined that the exfiltrated PII included AFTRA Health Plan's participants' name, address, Social Security number, AFTRA Number, date of birth, date of death, and "Past Information about: eligibility, dependent(s), claims, earnings, contributions, and beneficiaries."[5]

24. Beginning on or about December 17, 2020, AFTRA sent consumers a *Notice of Data Breach*. AFTRA informed the recipients of the notice that:

> On October 28, 2019, AFTRA received an alert of suspicious activity in its environment. AFTRA immediately launched an investigation into the nature and scope of the incident. As part of the investigation, which was conducted with the assistance of a third-party forensic specialist, it was determined that certain files and folders on AFTRA's network may have been subject to unauthorized access for periods of time between October 24, 2019 and October 28, 2019. AFTRA notified the media and placed notice of the incident on its website on February 25, 2020. Following these notices, AFTRA continued to review the files that may have been subject to unauthorized access to assess who could be impacted. AFTRA does not have evidence that files containing your information were accessed; however, access to these files could not be ruled out. AFTRA's internal review of the files and folders was time consuming and completed on September 25, 2020.[6]

25. AFTRA admitted in the *Notice of Data Breach* and the letters to the Attorneys General that their systems were subjected to unauthorized access for up to five days, and there is no indication that the exfiltrated PII was encrypted or retrieved. AFTRA further admitted that the unencrypted PII included name, address, date of birth and Social Security number.[7]

26. In response to the Data Breach, AFTRA claims:

> AFTRA takes this incident and the security of information in its care very

[5] AFTRA's *Notice of Data Privacy Event*, dated February 25, 2020, *available at*: https://aftraretirement.org/Home/news_updates/news_announcements/2020/02/25/notice-of-data-privacy-event.

[6] *See* AFTRA's *Notice of Data Breach*, filed Dec. 16, 2020 with the Washington Attorney General, *available at*: https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/AFTRARetirementFundUpdated.2020-12-16.pdf.

[7] *Id*.

> seriously. AFTRA is reviewing its existing security measures and working to implement additional safeguards to prevent similar incidents from occurring in the future. AFTRA will also notify the Office of Civil Rights at the Department of Health and Human Services and any required state or federal regulators regarding this incident.

27. AFTRA did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for current and former participants in the AFTRA Retirement Fund, causing Plaintiffs' and Class Members' PII to be exposed.

Securing PII and Preventing Breaches

28. AFTRA could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and computer files containing PII. And, as AFTRA claims it does, it should have taken the "appropriate physical, electronic, and other security measures to help safeguard personal information from unauthorized access, alteration, or disclosure."

29. AFTRA has acknowledged the sensitive and confidential nature of the PII. To be sure, collection, maintaining, and protecting PII is vital to many of AFTRA's business purposes. AFTRA 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.[8] 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, AFTRA failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

[8] For example, in the June 2019 AFTRA Retirement Plan Summary Plan Description, available on its website, AFTRA states that "[s]ince privacy laws limit how we may share your information, whenever you update your contact information, you must notify the AFTRA Retirement Fund directly — separate from any notifications you send to SAG-AFTRA, the SAG-Producers Pension Plan, the SAG-AFTRA Health Plan and other organizations." https://www.aftraretirement.org/docs/default-source/default-document-library/2019_aftra-retirement-fund_spd_rev-b_new-final_w-nav-links.pdf?sfvrsn=0

30. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[9] 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."[10]

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

Value of Personal Identifiable Information

32. 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.[11] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13]

33. 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

[9] 17 C.F.R. § 248.201 (2013).
[10] *Id*.
[11] *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/.
[12] *Here's How Much Your Personal Information Is Selling for on the Dark Web,* Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
[13] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

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.[14]

34. What is 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.

35. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The 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."[15]

36. 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. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, name, date of birth, address, and potentially other financial information.

---

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

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

37. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[16]

38. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

39. The fraudulent activity resulting from the Data Breach may not come to light for years.

40. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

41. At all relevant times, AFTRA knew, or reasonably should have known, of the importance of safeguarding its current and former consumers' PII, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if AFTRA's data security system was breached, including, specifically, the significant costs that would be imposed on AFTRA's consumers as a result of a breach.

42. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

---

[16] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[17] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf.

43. AFTRA was, or should have been, fully aware of the unique type and the significant volume of data on AFTRA's systems, amounting to thousands of individuals' detailed, personal, information and thus, the significant number of individuals who would be harmed by the loss of unencrypted data.

44. To date, AFTRA has offered its consumers only one year of identity monitoring service, with no identity theft insurance. The offered services are inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

45. The injuries to Plaintiffs and Class Members were directly and proximately caused by AFTRA's failure to implement or maintain adequate data security measures for its current and former retirement plan participants' PII.

AFTRA Failed to Comply with FTC Guidelines

46. 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.[18]

47. 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.[19] 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.

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

[19] 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

48. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[20]

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

50. AFTRA was at all times fully aware of its obligation to protect the personal and financial data of consumers, including Plaintiffs and members of the Classes. AFTRA was also aware of the significant repercussions if it failed to do so.[21]

51. AFTRA's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiffs' and Class Members' Social Security numbers, dates of birth, 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.

AFTRA's Data Breach Caused Harm and will Result in Further Harm

52. The ramifications of AFTRA's failure to keep Plaintiffs' and Class members' data secure are severe.

53. Consumer victims of data breaches are much more likely to become victims of identity fraud. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.[22]

---

[20] FTC, *Start With Security*, *supra* note 18.

[21] SAG-AFTRA is no stranger to data breaches. Its members received a data breach notice from SAG-AFTRA back in December 2014, warning them of a "security breach" that affected the data of individuals receiving payments through the ART payroll system. www.sagaftra.org/important-announcement-about-art-payroll

[22] 2014 LexisNexis True Cost of Fraud Study, https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

54. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[23] 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."[24]

55. PII is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[25]

56. Identity thieves can use personal information, such as that of Plaintiffs and members of the classes, which AFTRA failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

57. Javelin Strategy and Research reports that identity thieves have stolen $112 billion from 2010 to 2016—which has certainly increased since with the proliferation of data breaches.[26]

58. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending

[23] 17 C.F.R § 248.201 (2013).
[24] *Id.*
[25] Federal Trade Commission, *Warning Signs of Identity Theft*, *available at*: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft.
[26] Javelin, *2016 Identity Fraud: Fraud Hits an Inflection Point* (February 2, 2016), *available a*t: https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point

an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[27]

59. An independent financial services industry research study conducted for BillGuard—a private enterprise that automates the consumer task of finding unauthorized transactions that might otherwise go undetected—calculated the average per-consumer cost of all unauthorized transactions at roughly US $215 per cardholder incurring these charges,[28] some portion of which could go undetected and thus must be paid entirely out-of-pocket by consumer victims of account or identity misuse. This figure is based on misuse of cardholder information, which is less valuable than the PII at issue here—including full names, dates of birth, Social Security numbers, and other information which can easily be used to open credit accounts and other financial accounts to perpetrate further fraud, increasing the amount of average damages.

60. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[29]

61. Thus, Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

---

[27] Victims of Identity Theft, 2014 (Sept. 2015) *available at*: http://www.bjs.gov/content/pub/pdf/vit14.pdf.

[28] Hadley Malcom, *Consumers rack up $14.3 billion in gray charges, research study commissioned for BillGuard by Aite Research, USA Today* (July 25, 2013), *available at*: https://www.usatoday.com/story/money/personalfinance/2013/07/25/consumers-unwanted-charges-in-billions/2568645/.

[29] GAO, Report to Congressional Requesters, at 29 (June 2007), *available at*: http://www.gao.gov/new.items/d07737.pdf.

Plaintiff A.A.'s Experience

62. On or about August 22, 2014, A.A. was a non-union actor hired onto a union project. He received a Taft Hartley waiver and was allowed to work on the project. A.A. and his father, Mr. Altes, were required to supply A.A.'s personal identifiable information to AFTRA, including but not limited to his name, address, date of birth and Social Security number to participate in the AFTRA Retirement Fund. A.A. did not become a union member following the project.

63. A.A. received the *Notice of Data Breach*, dated December 17, 2020, on or about that date. It was addressed to the "Parent of Guardian of [A.A.]," which is Mr. Altes.

64. As a result of the Data Breach notice, Mr. Altes spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach*, communicating with AFTRA representatives, exploring credit monitoring and identity theft insurance options, signing up for the credit monitoring supplied by AFTRA, reporting the breach to the IRS and FTC, and self-monitoring accounts related to A.A. This time has been lost forever and cannot be recaptured.

65. Mr. Altes and A.A. are very careful about sharing PII, and have never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

66. Mr. Altes and A.A. store any and all documents containing PII in a safe and secure location, and destroy any documents they receive in the mail that contain any PII, or that may contain any information that could otherwise be used to compromise their credit card accounts and identity. Moreover, they diligently choose unique usernames and passwords for their various online accounts.

67. Mr. Altes and A.A. suffered actual injury and damages in paying money to AFTRA for facilitating the Retirement Fund before the Data Breach; expenditures which they would not have made had AFTRA disclosed that it lacked data security practices adequate to safeguard PII.

68. Mr. Altes and A.A. suffered actual injury in the form of damages to and diminution in the value of their PII—a form of intangible property that they entrusted to AFTRA for the

purpose of facilitating the Retirement Fund, which was compromised in and as a result of the Data Breach.

69. Mr. Altes and A.A. suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and have anxiety and increased concerns for the loss of their privacy, especially A.A.'s Social Security number.

70. Mr. Altes and A.A. have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from A.A.'s PII, especially their Social Security numbers, being placed in the hands of unauthorized third-parties and possibly criminals.

71. Mr. Altes and A.A. have a continuing interest in ensuring that A.A.'s PII, which, upon information and belief, remains backed up in AFTRA's possession, is protected and safeguarded from future breaches.

Plaintiff Bright's Experience

72. From approximately 1982 to 2006, Plaintiff Paul Bright was a union member working as an actor. In or about 2006 he elected financial core status. This made him ineligible to draw retirement funds. Mr. Bright, however, had not worked enough years to be vested in the retirement funds. Mr. Bright was required to supply his personal identifiable information to AFTRA, including but not limited to his name, address, date of birth and Social Security number to participate in the AFTRA Retirement Fund.

73. Mr. Bright received the *Notice of Data Breach*, dated December 17, 2020, on or about that date.

74. As a result of the Data Breach notice, Mr. Bright spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach*, communicating with AFTRA representatives, exploring credit monitoring and identity theft insurance options, signing up for the credit monitoring supplied by AFTRA, reporting the breach to the IRS, placing security freezes with all three credit bureaus, and self-monitoring his accounts. Mr. Bright also took AFTRA's recommendation and contacted the FTC. He reported

the Data Breach to the FTC and on the FTC's recommendation, he is preparing to file his taxes early because his Social Security number was stolen in the breach. This time has been lost forever and cannot be recaptured.

75. Mr. Bright is very careful about sharing his PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

76. Mr. Bright stores any and all documents containing PII in a safe and secure location, and destroys any documents he receives in the mail that contain any PII, or that may contain any information that could otherwise be used to compromise their credit card accounts and identity. Moreover, he diligently chooses unique usernames and passwords for their various online accounts.

77. Mr. Bright suffered actual injury and damages in paying money to AFTRA for facilitating the Retirement Fund before the Data Breach; expenditures which he would not have approved had AFTRA disclosed that it lacked data security practices adequate to safeguard PII.

78. Mr. Bright suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to AFTRA for the purpose of facilitating the Retirement Fund, which was compromised in and as a result of the Data Breach.

79. Mr. Bright suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and have anxiety and increased concerns for the loss of his privacy.

80. Mr. Bright has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security numbers, being placed in the hands of unauthorized third-parties and possibly criminals.

81. Mr. Bright has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in AFTRA's possession, is protected and safeguarded from future breaches.

Plaintiff Choi's Experience

82. Billy Choi joined the SAG-AFTRA union in or about 2013 and is a member in good standing. Mr. Choi was required to supply his personal identifiable information to AFTRA, including but not limited to his name, address, date of birth and Social Security number to participate in the AFTRA Retirement Fund.

83. Mr. Choi received the *Notice of Data Breach*, dated December 17, 2020, on or about that date.

84. As a result of the Data Breach notice, Mr. Choi spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach*, exploring credit monitoring and identity theft insurance options, signing up for the credit monitoring supplied by AFTRA, reporting the breach to the IRS and FTC, placing security freezes with all three major credit bureaus, "locking" all of his credit card accounts, and self-monitoring accounts. This time has been lost forever and cannot be recaptured.

85. Mr. Choi is very careful about sharing his PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

86. Mr. Choi stores any and all documents containing PII in a safe and secure location, and destroys any documents he receives in the mail that contain any PII, or that may contain any information that could otherwise be used to compromise their credit card accounts and identity. Moreover, he diligently chooses unique usernames and passwords for their various online accounts.

87. Mr. Choi suffered actual injury and damages in paying money to AFTRA for facilitating the Retirement Fund before the Data Breach; expenditures which he would not have made had AFTRA disclosed that it lacked data security practices adequate to safeguard PII.

88. Mr. Choi suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to AFTRA for the purpose of facilitating the Retirement Fund, which was compromised in and as a result of the Data Breach.

89. Mr. Choi suffered lost time, annoyance, interference, and inconvenience as a result

of the Data Breach and have anxiety and increased concerns for the loss of his privacy.

90. Mr. Choi has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security numbers, being placed in the hands of unauthorized third-parties and possibly criminals.

91. Mr. Choi has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in AFTRA's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

92. Plaintiffs bring this nationwide class action on behalf of themselves 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.

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

> All persons residing in the United States whose PII was compromised in the data breach announced by AFTRA on or about December 17, 2020 (the "Nationwide Class").

94. The California Subclass is defined as follows:

> All persons residing in California whose PII was compromised in the data breach announced by AFTRA on or about December 17, 2020 (the "California Subclass").

95. The Oregon Subclass is defined as follows:

> All persons residing in Oregon whose PII was compromised in the data breach announced by AFTRA on or about December 17, 2020 (the "Oregon Subclass").

96. The above classes and subclasses are herein referred to as the "Classes."

97. Excluded from the Classes are the following individuals and/or entities: AFTRA and AFTRA's parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which AFTRA 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.

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

99. Numerosity, Fed R. Civ. P. 23(a)(1): Classes are so numerous that joinder of all members is impracticable. AFTRA has identified thousands of consumers whose PII may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within AFTRA's records.

100. 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 AFTRA had a duty to protect the PII of Plaintiffs and Class Members;
b. Whether AFTRA had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;
c. Whether AFTRA had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;
d. Whether AFTRA failed to adequately safeguard the PII of Plaintiffs and Class Members;
e. Whether and when AFTRA actually learned of the Data Breach;
f. Whether AFTRA adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;
g. Whether AFTRA violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;
h. Whether AFTRA failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

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

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

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

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of AFTRA's wrongful conduct;

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

n. Whether AFTRA violated the California Unfair Competition Law, California Business & Professions Code § 17200, *et seq.*;

o. Whether AFTRA violated the Oregon Unlawful Trade Practices Act, Or. Rev. Stat. §§ 646.608, *et seq*.

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

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

103. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that

is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously.

104. 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 AFTRA. 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.

105. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because AFTRA would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were 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.

106. The litigation of the claims brought herein is manageable. AFTRA'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.

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

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

109. Further, AFTRA 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.

110. 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 AFTRA owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
b. Whether AFTRA breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
c. Whether AFTRA 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 AFTRA on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;
e. Whether AFTRA breached the implied contract;
f. Whether AFTRA adequately, and accurately informed Plaintiffs and Class Members that their PII had been compromised;
g. Whether AFTRA 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 AFTRA engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs 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 AFTRA's wrongful conduct.

VI. APPLICATION OF NEW YORK LAW TO THE NATIONWIDE CLASSES

111. The laws of New York should govern Plaintiffs' claims and, therefore, the claims of the Nationwide Classes that Plaintiffs seek to represent.

112. AFTRA is headquartered at 261 Madison Avenue, 7th floor, New York, New York. Upon information and belief, the headquarters is the "nerve center" of AFTRA's business activities—the place where its executive-level and similarly-responsible officers, directors, and other high-level employees direct, control, and coordinate the corporation's activities, including its data security functions and major policy and legal decisions.

113. New York has a significant interest in regulating the conduct of businesses operating within its borders. New York, which seeks to protect the rights and interests of residents and citizens of the United States against financial companies headquartered and doing business in New York, has a greater interest in the nationwide claims of Plaintiffs and members of the Classes than any other state and is mot intimately concerned with the claims and outcome of this litigation.

114. Upon information and belief, all contracts that Plaintiffs and members of the classes reviewed and executed were created by AFTRA in New York.

115. Upon information and belief, all monies that Plaintiffs and members of the classes made to AFTRA were ultimately delivered to AFTRA in New York.

116. Upon information and belief, AFTRA's response to the Data Breach, and the decisions and responses thereto, were made from and in New York.

117. Application of New York law to Plaintiffs' and members of the classes claims would be neither arbitrary nor fundamentally unfair because New York has a significant interest in the claims of Plaintiffs and members of the Classes.

118. Under choice of law principles applicable to this litigation, the common law of New York would apply to the nationwide common law claims, as well as the New York law claims, of all class members because New York's significant interest in regulating the conduct of businesses—AFTRA included—operating within its borders. Thus, New York's consumer protection laws may be applied to non-resident consumers across the United States.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class, or in the alternative, on behalf of the Subclasses)

119. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 118.

120. As a condition of their using the services of AFTRA, consumers were obligated to provide AFTRA with certain PII, including their name, date of birth, address, and Social Security number.

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

122. AFTRA has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

123. AFTRA 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 Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

124. AFTRA 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 AFTRA's security protocols to ensure that Plaintiffs' and Class Members' information in AFTRA's possession was adequately secured and protected.

125. AFTRA also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' PII.

126. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class Members was reasonably foreseeable, particularly in light of AFTRA's inadequate security practices and previous breach incidents involving AFTRA consumers' PII on stolen equipment.

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

128. AFTRA's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. AFTRA'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. AFTRA's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiffs' and Class Members' PII, including basic encryption techniques freely available to AFTRA.

129. Plaintiffs and the Class Members had no ability to protect their PII that was in, and possibly remains in, AFTRA's possession.

130. AFTRA was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

131. AFTRA had and continues to have a duty to adequately disclose that the PII of Plaintiffs and Class Members within AFTRA'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 Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

132. AFTRA had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and Class Members.

133. AFTRA has admitted that the PII of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

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

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

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

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

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

139. But for AFTRA's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII of Plaintiffs and Class Members would not have been compromised.

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

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

142. AFTRA violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. AFTRA's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

143. AFTRA's violation of Section 5 of the FTC Act constitutes negligence *per se*.

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

145. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

146. As a direct and proximate result of AFTRA's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity 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 AFTRA's possession and is subject to further unauthorized disclosures so long as AFTRA 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 Plaintiffs and Class Members; and (ix) the diminished value of AFTRA's goods and services they received.

147. As a direct and proximate result of AFTRA's negligence, Plaintiffs 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.

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

COUNT II
Breach of Confidence
(On Behalf of Plaintiffs and the Nationwide Class, or in the alternative, on behalf of the Subclasses)

149. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 118.

150. At all times during Plaintiffs' and Class Members' interactions with AFTRA, AFTRA was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' PII that Plaintiffs and Class Members provided to AFTRA.

151. As alleged herein and above, AFTRA's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

152. Plaintiffs and Class Members provided their respective PII to AFTRA with the explicit and implicit understandings that AFTRA would protect and not permit the PII to be disseminated to any unauthorized third parties.

153. Plaintiffs and Class Members also provided their respective PII to Defendant with the explicit and implicit understandings that AFTRA would take precautions to protect that PII from unauthorized disclosure.

154. AFTRA voluntarily received in confidence Plaintiffs' and Class Members' PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

155. Due to AFTRA's failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

156. As a direct and proximate cause of AFTRA's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

157. But for AFTRA's disclosure of Plaintiffs' and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. AFTRA's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting damages.

158. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of AFTRA's unauthorized disclosure of Plaintiffs' and Class Members' PII. AFTRA knew or should have known its methods of accepting and securing Plaintiffs' and Class Members' PII was inadequate as it relates to, at the very least, disposal of servers and other equipment containing Plaintiffs' and Class Members' PII.

159. As a direct and proximate result of AFTRAs' breach of its confidence with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses

associated with the prevention, detection, and recovery from identity theft, 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 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; (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 Plaintiffs and Class Members; and (ix) the diminished value of AFTRA's goods and services they received.

160. As a direct and proximate result of Defendant's breaches of confidence, 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.

COUNT III
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful Business Practices
(On Behalf of Plaintiffs A.A. and Choi and the California Subclass)

161. Plaintiffs A.A. and Choi (the "Plaintiffs" for this count) re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 118.

162. AFTRA has violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the California Class.

163. AFTRA engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and California Subclass Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and California Subclass Members' PII in an unsecure environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires AFTRA to take reasonable methods of safeguarding the PII of Plaintiffs and the California Subclass Members.

164. In addition, AFTRA engaged in unlawful acts and practices by failing to disclose the Data Breach to California Subclass Members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

165. As a direct and proximate result of AFTRA's unlawful practices and acts, Plaintiffs and the California Subclass Members were injured and lost money or property, including but not limited to the price received by AFTRA for the services, the loss of California Subclass Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

166. AFTRA knew or should have known that AFTRA's computer systems and data security practices were inadequate to safeguard California Subclass Members' PII and that the risk of a data breach or theft was highly likely, especially given AFTRA's inability to adhere to basic encryption standards and data disposal methodologies. AFTRA's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Subclass.

167. California Subclass Members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiffs and California Subclass Members of money or property that AFTRA may have acquired by means of AFTRA's unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to AFTRA because of AFTRA's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT IV
Violation of California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*. – Unfair Business Practices
(On Behalf of Plaintiffs A.A. and Choi and the California Subclass)

168. Plaintiffs A.A. and Choi (the "Plaintiffs," for this count) re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 118.

169. AFTRA engaged in unfair acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and California Subclass Members' PII with knowledge that the information would not be adequately protected; by storing Plaintiffs' and California Subclass Members' PII in an unsecure electronic environment; and by failing to properly dispose of equipment containing sensitive PII. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Subclass Members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiffs and the California Subclass Members outweighed their utility, if any.

170. AFTRA engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect California Subclass Members' PII from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Subclass Members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiffs and the California Subclass Members outweighed their utility, if any.

171. As a direct and proximate result of AFTRA's acts of unfair practices, Plaintiffs and the California Subclass Members were injured and lost money or property, including but not limited to the price received by AFTRA for the services, the loss of California Subclass Members'

legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

172. AFTRA knew or should have known that AFTRA's computer systems and data security practices were inadequate to safeguard California Subclass Members' PII and that the risk of a data breach or theft was highly likely, including AFTRA's failure to properly encrypt and dispose of equipment containing sensitive PII. AFTRA's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Subclass.

173. California Subclass Members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiffs and California Subclass Members of money or property that AFTRA may have acquired by means of AFTRA's unfair business practices, restitutionary disgorgement of all profits accruing to AFTRA because of AFTRA's unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT V
Violations of the Oregon Unlawful Trade Practices Act,
(Or. Rev. Stat. §§ 646.608, *et seq*.)
(On Behalf of Plaintiff Bright and the Oregon Subclass)

174. Plaintiff Bright, individually and on behalf of the other Oregon Subclass members, re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 118.

175. AFTRA is a "person," as defined by Or. Rev. Stat. § 646.605(4).

176. AFTRA engaged in the sale of "goods and services," as defined by Or. Rev. Stat. § 646.605(6)(a).

177. AFTRA sold "goods or services," as defined by Or. Rev. Stat. § 646.605(6)(a).

178. AFTRA advertised, offered, or sold goods or services in Oregon and engaged in

trade or commerce directly or indirectly affecting the people of Oregon.

179. AFTRA engaged in unlawful practices in the course of its business and occupation, in violation of Or. Rev. Stat. § 646.608, included the following:

a. Represented that its goods and services have approval, characteristics, uses, benefits, and qualities that they do not have, in violation of Or. Rev. Stat. § 646.608(1)(e);

b. Represented that its goods and services are of a particular standard or quality if they are of another, in violation of Or. Rev. Stat. § 646.608(1)(g);

c. Advertised its goods or services with intent not to provide them as advertised, in violation of Or. Rev. Stat. § 646.608(1)(i); and

d. Concurrent with tender or delivery of its goods and services, failed to disclose any known material defect, in violation of Or. Rev. Stat. § 646.608(1)(t).

180. AFTRA's unlawful practices include:

e. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Bright and Oregon Subclass members' PII, which was a direct and proximate cause of the Data Breach;

f. 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, which was a direct and proximate cause of the Data Breach;

g. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*, which was a direct and proximate cause of the Data Breach;

h. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Bright and Oregon Subclass members' PII, including by implementing and

maintaining reasonable security measures;

i. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Bright and Oregon Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq*.;

j. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Bright and Oregon

k. 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 Plaintiff Bright and Oregon Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq*.

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

182. AFTRA intended to mislead Plaintiff Bright and Oregon Subclass members and induce them to rely on its misrepresentations and omissions. Had AFTRA disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, AFTRA 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, AFTRA received, maintained, and compiled Plaintiff Bright's and Class members' PII as part of the services AFTRA provided and for which Plaintiff and Class members paid without advising Plaintiff and Class members that AFTRA's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff Garrison's and Class members' PII. Accordingly, Plaintiff Bright and the Oregon Subclass members acted reasonably in relying on AFTRA's misrepresentations and omissions, the

truth of which they could not have discovered.

183. AFTRA acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act, and recklessly disregarded Plaintiff and Oregon Subclass members' rights. Recent, frequent, and strikingly similar data breaches within the industry put AFTRA on notice that its security and privacy protections were inadequate.

184. As a direct and proximate result of AFTRA's unlawful practices, Plaintiff Bright and Oregon Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with AFTRA as they would not have paid AFTRA for goods and services or would have paid less for such goods and services but for AFTRA's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

185. Plaintiff Bright and Oregon Subclass members seek all monetary and non-monetary relief allowed by law, including equitable relief, restitution, actual damages or statutory damages of $200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, requests judgment against the AFTRA and that the Court grant the following:

A. For an Order certifying the Nationwide Classes or, in the alternative, the Subclasses as defined herein, and appointing Plaintiffs and their Counsel to represent the certified Classes;

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

disclosures to the Plaintiffs and Class members;

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

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

ii. requiring AFTRA 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 AFTRA to delete, destroy, and purge the personal identifying information of Plaintiffs and class members unless AFTRA can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and class members;

iv. requiring AFTRA to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs and class members' personal identifying information;

v. prohibiting AFTRA from maintaining Plaintiffs' and class members' personal identifying information on a cloud-based database;

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

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

viii. requiring AFTRA to audit, test, and train its security personnel regarding any

new or modified procedures;

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

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

xi. requiring AFTRA 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 Plaintiffs and class members;

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

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

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

xv. requiring AFTRA 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 AFTRA to implement logging and monitoring programs sufficient to track traffic to and from AFTRA'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 AFTRA'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, 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

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

Date: December 31, 2020

Respectfully Submitted,

/s/ *Amanda Peterson*
AMANDA PETERSON (AP1797)
MORGAN & MORGAN
90 Broad Street, Suite 1011
New York, NY 10004
(212) 564-4568
apeterson@ForThePeople.com

JOHN A. YANCHUNIS
(*Pro Hac Vice application forthcoming*)
RYAN J. MCGEE
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor

Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

M. ANDERSON BERRY
(*Pro Hac Vice application forthcoming*)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
(916) 777-7777
aberry@justice4you.com